哥本哈根 — 联合会议：ICANN 董事会和技术专家小组 (TEG)
欧洲中部时间 2017 年 3 月 15 日（星期三）— 17:00 至 18:30
ICANN58 | 丹麦哥本哈根

史蒂夫 • 康特
(STEVE CONTE)： 如果有人在找普遍适用性小组的话，它已经从这间会议室转移到 B5.1 了。不是我们不要你们在这里，如果你们要参加的不是 TEG 会议，而是普遍适用性会议的话，那么应该去 B5.1。现在我要开动战舰了。

戴维 • 康纳德
(David Conrad)： 什么 — 噢，哇哦。派对可以开始了。琼尼在这里。

>> （不在麦克风前。）

戴维 • 康纳德： 实际上，我们现在还在做一些后勤变动。史蒂夫和露丝薇斯说他们正在路上，所以他们一会就能到。我们正在尝试调整一些幻灯片。

>> （不在麦克风前。）

戴维 • 康纳德： 是的，实际上，如果大家喜欢的话，我们可以先开始一些介绍。就背景而言，这是董事会与技术专家之间的会议，类似于铁笼赛。好的。可能不是。

这是 — 我不知道，一些技术专家小组会议。是为了让技术专家向董事会提供意见。我们不提供建议，而是提供意见。这是 — 最初，它是个封闭性会议，但自从开放后，我们就欢迎那些对令人讨厌的东西感兴趣的人来参加。

我们来看看。是否 — 大家知道，显然有一个问题 — 是否，大家知道，是否邀请了 RSSAC 和 SSAC。那么，(a) 这是个开放性会议，(b) 可能有一些疑惑，因为我们 — 是哪次会议来着？马拉喀什会议？我忘记是哪次会议了，但那时我们不得不 — 我们不得不取消 TEG 来做一些移交相关的事务，所以我们没有开 TEG 会议，而是决定召开 TEG/董事会鸡尾酒会，这是为了稍微提高一点趣味性，我们还邀请了 RSSAC 和 SSAC，所以说那是一场董事会/TEG/SSAC/RSSAC 鸡尾酒会，现在这有点变成了一种准传统，也就是说，我们欢迎 TEG 成员和董事会成员加入 TE — 今天晚上 7:00 在红宝石厅举行的鸡尾酒会，诸如此类。

>> 7:00。

戴维 • 康纳德： 7:00，巴士 6:45 离开，在前面 —

实际上，你有麦克风。

>> 会后 6:45，我们有一个穿梭巴士，一个相当大的穿梭巴士，在贝拉中心，西入口，就在这里的拐角处。

6:45，请进来加入我们。谢谢。

戴维 • 康纳德： 史蒂夫来了，琼尼也在，那么派对可以开始了。

>> （不在麦克风前。）

戴维 • 康纳德： 是的。你想说点什么吗？

史蒂夫 • 克罗克 (Steve Crocker)： 当然。抱歉来晚了。看到这么多人在这里，我非常高兴。这太好了。戴维是负责人。

[笑声]

戴维 • 康纳德： 好的。那么我们先从介绍开始。

马克，如果你愿意的话。你的姓名，公司，最喜欢的颜色。我不知道。

马克 • 布兰切特
(MARC BLANCHET)： 马克 • 布兰切特。

杰 • 戴利 (JAY DALEY)： 杰 • 戴利，.NZ。

丹尼尔 • 达戴勒
(DANIEL DARDAILLER)： 丹尼尔 • 达戴勒，W3C。

利托 • 伊瓦拉
(LITO IBARRA)： 利托 • 伊瓦拉，ICANN 董事会。

卡韦赫 • 兰杰巴尔
(Kaveh Ranjbar)： 卡韦赫 • 兰杰巴尔，技术人员和 ICANN 董事会成员。

拉斯 • 约翰 • 利曼

(LARS JOHAN-LIMAN)： 拉斯 • 约翰 • 利曼，Netnod 的根服务器运营负责人。

乔治 • 萨多夫斯基

(GEORGE SADOWSKY)： 乔治 • 萨多夫斯基，ICANN 董事会。

里纳利亚 • 阿卜杜尔 • 拉辛

(RINALIA ABDUL RAHIM)： 里纳利亚 • 阿卜杜尔 • 拉辛，ICANN 董事会。

帕特里克 • 弗斯特朗姆

(Patrik Faltstrom)： 帕特里克 • 弗斯特朗姆，SSAC 主席。

阿什文 • 兰根

(Ashwin Rangan)： 阿什文 • 兰根，ICANN 员工。

谢林 • 查拉比

(Cherine Chalaby)： 谢林 • 查拉比，ICANN 董事会。

马库斯 • 库墨
(Markus Kummer)： 马库斯 • 库墨，ICANN 董事会。

特里 • 曼德尔森
(Terry Manderson)： 特里 • 曼德尔森，ICANN 工作人员，DNS 工程部主管，IETF 互联网领域的区域主管。

阿兰 • 杜朗德
(Alain Durand)： 阿兰 • 杜朗德，ICANN 员工，OCTO 研究。

阿莎 • 合美嘉妮
(ASHA HEMRAJANI)： 阿莎 • 合美嘉妮，ICANN 董事会。

保罗 • 维克西 (AUL VIXIE)： 保罗 • 维克西，保罗 • 维克西，受邀嘉宾。

杰里米 • 兰特
(JEREMY RAND)： 杰里米 • 兰特，Namecoin 项目。

保罗 • 胡特斯
(PAUL WOUTERS)： 保罗 • 胡特斯，IETF 联络人。

史蒂夫 • 克罗克： 史蒂夫 • 克罗克，ICANN 董事会。

戴维 • 康纳德： 戴维 • 康纳德，ICANN 组织。

史蒂夫 • 康特
(STEVE CONTE)： 史蒂夫 • 康特，ICANN 组织员工。

凯西 • 彼得森
(Cathy Peterson)： 凯西 • 彼得森，ICANN 组织员工。

温迪 • 普若菲特
(Wendy Profit)： 温迪 • 普若菲特，ICANN 组织员工。

琼尼 • 索尼能
(JONNE SOININEN)： 琼尼 • 索尼能，IETF 的 ICANN 董事会联络人。

丹 • 约克 (DAN YORK)： 丹 • 约克，国际互联网协会，重点关注 DNSSEC。

苏珊 • 沃尔夫
(Suzanne Woolf)： 苏珊 • 沃尔夫，SSAC，RSSAC，随机的麻烦制造者。

沃伦 • 库马里
(WARREN KUMARI)： 沃伦 • 库马里，IETF 联络人。

爱德华 • 刘易斯
(ED Lewis)： 爱德华 • 刘易斯，ICANN 组织，OCTO 研究。

罗伊 • 阿伦兹
(Roy Arends)： 罗伊 • 阿伦兹，ICANN OCTO 研究。

迈特 • 拉森
(Matt Larson)： 迈特 • 拉森，同样来自 OCTO ICANN 研究。

弗朗西斯科 • 达席尔瓦

(FRANCISCO DA SILVA)： 弗朗西斯科 • 达席尔瓦，来自 ETSI，我的公司是全球性的瑞典公司。

霍华德 • 本

(HOWARD BENN)： 霍华德 • 本，同样代表 ETSI。

朱莉 • 翰墨

(JULIE HAMMER)： 朱莉 • 翰墨，SSAC。

罗德 • 拉斯穆森

(ROD RASMUSSEN)： 罗德 • 拉斯穆森，SSAC。

>> （说名字）来自 ITU-T。

阿迪尔 • 阿科普罗根

(Adiel Akplogan)： 阿迪尔 • 阿科普罗根，ICANN 组织工作人员，技术合作部。

格雷格 • 亚伦
(GREG AARON)： 格雷格 • 亚伦，SSAC。

玛盾 • 波特曼
(Maarten Botterman)： 玛盾 • 波特曼，ICANN 董事会。

亚普 • 阿克休伊斯
(JAAP AKKERHUIS)： 亚普 • 阿克休伊斯，SSAC 和 RSSAC 决策委员会。

露丝薇斯 • 范德朗
(Lousewies van der Laan)： 抱歉来晚了。露丝薇斯 • 范德朗，ICANN 董事会。

约翰 • 克雷恩
(JOHN CRAIN)： 我刚才躲在后面，认为我应该到前面去。约翰 • 克莱恩，ICANN 组织，SSR 首席官员。

戴维 • 康纳德： 好的。非常感谢。

那么，议程已经在屏幕上了。这是一次欢迎和管理会议。

我想重申一下刚才的话，如果你们在找普遍适用性指导小组会议，它已经转移到 B5.1 了，就在走廊下面。但我们仍然欢迎你们参加这个会议。当然，这是技术专家小组与董事会的铁笼赛。

我们继续，我想我们先让 Namecoin 项目的杰里米 • 兰特讲一下 Namecoin。杰里米，请你开个头。

杰里米 • 兰特： 大家好。我是来自 Namecoin 的杰里米 • 兰特，那么我们开始吧。

首先是全面披露。我是最活跃的 Namecoin 开发人员之一，据我所知，没有哪个 Namecoin 开发人员不同意这次演讲中的任何内容。但我不能在所有事务上代表所有的开发人员。我们是一个开源项目，并没有清晰的组织结构，所以要注意这一点。

这次演讲是与雨果 • 兰道 (Hugo Landau) 合作准备的。

因此，Namecoin 的潜在动机是人类行为的非确定性性，延伸来讲，任何由人类运行的系统都会表现出非确定性。

特别是，即使某个系统具有本应不可违反的基本规则，但由人类执行的基本规则的执行情况也会有不一致之处。

举例来说，美国宪法设置了基本规则，禁止折磨和大量监控。遗憾的是，这些基本规则是由人类执行的，因此，我们都知道，这些规则在任何地方都没有像我们希望的那样得到确定性的执行。

而在遥远的未来，人类的行为更加不确定。

例如，预测选举结果在未来将进一步变得更加困难，因此，预测一个国家的政治气候在将来也会更加困难。

DNS 在很大程度上是由人类来运行的。这就会造成风险，因为参与运营 DNS 的人员可能会表现出非确定性。

也许你的注册服务机构犯了一个错误，让别人更改了你的记录，或者也许拥有你的 ccTLD 的政府可能会在 10 年后被推翻，新的政府不喜欢你的名称，并决定将其没收，或者也许在政治压力下，ICANN 未来可能会实施你现在不认同的新政策。

所有这些都有可能发生，令人担忧。

那么，Namecoin 是一个实验，目的是探索是否有可能构建一些类似于 DNS 的东西，但尽可能减少人为参与，从而创建一个类 DNS 系统，但其行为比 DNS 更具确定性。我们希望，像这样的系统能够更具可靠性，更能抵御人类造成的故障模式，因为这种系统更具确定性。

那么我们来看看一些现有的标识符系统，看看它们如何与 Namecoin 相比。

一个站点的人工命名，比如主机文件，它们没有全球域名空间，这意味着这些名称只在本地有意义，但是它们不受非确定性的人类第三方影响，并且具有对人类有意义的名称，所以这很好。

诸如 DNS 之类的层级命名具有全球域名空间，但是会受到非确定性的人类第三方影响。它确实有对人类有意义的名称。这具有非常好的可用性，但作为信任根，它具有危险性。

像 BitTorrent 这样的内容寻址，其名称是拼凑而成的，具有全球域名空间，并且不受非确定性人类第三方影响，但它没有对人类有意义的名称，而且内容永远不能改变。

如果名称是公共密钥，情况就有所不同。例如 Tor 使用的 .ONION 域名。这些名称具有全球域名空间，并且不受非确定性人类第三方影响，但它同样没有对人类有意义的名称。但内容可以更改。这类系统作为信任根是安全的，但可用性极差。用户尝试输入内容时，会看到一个 URL，和大家在屏幕上看到的一样。

其实我在说谎。Tor 正在进行安全升级，升级完成后，名字实际上看起来是这样的。

[笑声]

杰里米 • 兰特： 是的。大家在之前的幻灯片中可能已经注意到有两个勾号和一个 X 号，这就是 Zooko 三角。所以，Zooko Wilcox 推测，不可能马上实现所有这三个方面。

接着讨论一个稍有不同的话题，为确保问责制，只能追加的公共日志越来越受欢迎。最成功的例子就是谷歌的证书透明度。在公共 Web 上使用的每个证书都被放入一个仅可追加日志中，最终，浏览器可能需要将证书记录为有效。即使你想控制某个系统，你可能也会希望发布所有操作。

证书透明度是一个用于证书的仅可追加日志，但它不是非常适合与 DNS 等系统一起使用，原因是谁可以写入日志？任何人都可以。但只有来自经认可的认证机构的证书才能写入。这有助于确保日志不会充斥着垃圾数据，但受信任实体的手动列表有点繁琐。

Namecoin 是用于名称注册和更新的仅可追加日志。但是，与证书透明度不同，Namecoin 是使用区块链来实施的，所以它可以通过强加写入数据的经济成本来来防止垃圾邮件，这个成本很小但非常有效，可以抑制操作不当者大量抢注名称，而无需依赖于受信任实体的手动列表。

Namecoin 具有全球域名空间，不受非确定性人类第三方影响，并且具有对人类有意义的名称，所以它是 Zooko 三角的解决方案。Namecoin 意味着用于命名的仅可追加日志可以作

为一个开放论坛运行，从而增强其实用性。因此，问责制和透明度可以成为可通过加密方式验证的公众利益。并且与 Namecoin 用于名称的规则系统无关的是，其作为仅可追加日志的性质意味着，如果有不当操作者做了什么事，你总会知情。

作为一个思考实验，考虑一个负责任的根区的想法。问责制可以让心存疑问的相关方相信并没有发生什么事。

举一个假设的例子，将根区作为一个仅可追加的日志进行维护，让全世界的国家都相信，即使在政府间层级，美国的控制权也没有被滥用。

根服务器可以直接从日志中提取。作为仅可追加的日志进行维护的根区能让各个国家相信，例如，他们的 ccTLD 不会因为政治原因而受到干扰，这有些类似于各国根据禁止核试验条约采用地震监测来相互检查，以确保和平。信任但要验证。要明确的是，我并不是建议在 DNS 中实施这种特殊理念，而是想说这是一个有趣的假设案例研究。

稍微转换一下话题，有一个相关的问题是 TLS 公钥基础设施。即使有证书透明度，目前使用的认证机构系统也是有问题的。其中基本的问题是，有太多非确定性人类参与其中，他们会犯错误。DNSSEC 和 DANE 在 DNS 中储存 TLS 数据，而不是让认证机构验证他们，可能会改善这一情况。遗憾的是，还存在一

些政治问题。一些人非常担心 DNS 根或 TLD 运营商滥用的可能性。

同样，这里的问题是，DNS 根和 TLD 运营商也都有人类参与。所以它没有完全解决人类参与的问题。Namecoin 可以提供 DNSSEC 和 DANE 在这方面的优势，而且没有政治问题。

我们并不期望大多数软件，甚至是大多数域名解析库直接知道 Namecoin。我们期望在本地直接安装 Namecoin 至 DNS 的桥接软件，将 DNS 查询转化为 Namecoin 查询，并将 Namecoin 响应转回至 DNS。

Namecoin 使用 .BIT 顶级域，目前还没有在 ICANN 或 IETF 注册。我们希望能找到一种可行的解决方式。我们意识到这是一个问题。例如，我们可以使用特殊用途域名注册机构，例如 Tor 的 .ONION。

我们将这种限制称为 NCDNS，其作用有点类似于在 localhost 上运行的 .BIT 顶级域的权威 DNS 服务器。DNSSEC 用户生成一个安装时间，而我们有意尝试将 Namecoin 的域名规范轻松地映射到 DNS，以便轻松使用桥接软件。

假设您想使用此功能，您可以告诉您的递归 DNS 服务器，例如，Unbound 将 NCDNS 用作 .BIT 的权威，并为之提供 NCDNS 的 DNSSEC 公钥。理论上，一切应该能够奏效。这只是 unbound.com 中的少数几个策略。

实际上，有一些 DNS 功能没有得到非常广泛的支持。例如，TLS 的 DANE。所以我们要做一些奇怪的乘法定制，让它奏效。实际上，我曾经尝试记录我们要使用多少层不同的疯狂巫术，来让 Namecoin 的 DNAE 工作对于不支持 TLS 的 DANE 的浏览器奏效。在数了五层巫术后，我停下来了。

那么，有哪些现实使用案例能表明 Namecoin 的确定性行为对我们有所帮助？比如说，你正在尝试购买或出售某个名称。在 DNS 中，购买或出售名称通常会涉及到一些对手方风险，您可能需要依靠代管代理来减轻对手方风险。

在 Namecoin，买方和卖方可以共同构建一项交易，以原子方式向卖方付款并将名称转让给买方。这样就消除了对手方风险，而不需要托管代理的服务。

这样很好，但如果买方和卖方甚至都不愿意相互交谈来设置原子交易呢？你可以购买或出售要约。工作流程是这样的。爱丽丝创建了一个销售要约。我想要以 100 域名币的价格出售域名 example.bit。爱丽丝用她的私钥签署了销售要约，证明她拥有 example.bit 并希望用它来换取 100 域名币。爱丽丝可以将这份已签署的销售要约发布在论坛上或 pastebin 上，或类似地方。

鲍勃看到这个要约，希望购买 example.bit。鲍勃可以用拥有 100 域名币的私钥来签署要约，从而完成要约。现在这个要约

就是有效的 Namecoin 交易了。鲍勃现在可以向 Namecoin 网络播放，不需要再次联系爱丽丝。

爱丽丝拿到了付款。鲍勃收到了域名。这个交易就是原子式的。没有对手方风险，也不需要托管代理。这对于购买要约和销售要约都适用。Namecoin 协议已经支持这种使用案例了，预计很快将会推出人性化的工具。

另外，另一个使用案例是，一个名称通常由一个私钥拥有，但是你也可以让它由多个私钥拥有，其中需要存在 M-of-N 密钥，以便发布更新。这可以有效地避免受到单个被盗密钥的影响。例如，一组董事会成员可能每个人有一个密钥，而更新名称可能需要董事会的绝大多数票。同样，Namecoin 协议也支持这种使用案例，预计很快将会推出人性化的工具。

Namecoin 还允许建立非常灵活的更新策略，可以用来根据安全性和名称拥有者的 UX 需要来进行定制。例如，爱丽丝拥有一个名称，但她希望限制她的私钥被盗的风险，同时不会引起太多的对手方风险。所以她构建了一个这样的策略：爱丽丝可以与特伦特签订合同，运行二元认证服务。然后如果特伦特签署了她的更新，爱丽丝可以用任意数据更新其名称。特伦特承诺在通过二元认证进行验证之后才这样做。

但此外，之后爱丽丝可能想要在特伦特没有批准的情况下做一些事情，那么特伦特可以为某些事件预先签署特定交易。例

如，也许爱丽丝可能希望能够撤销她的 TLSA 记录，这样如果她的 Web 服务器被盗用，她就可以轻松地撤销证书。或者爱丽丝可能担心特伦特可能会消失或者停业或者失去其私钥。所以可以根据可定制的限制来指定这些策略。没有爱丽丝的签名，特伦特就没法转让或更新爱丽丝的名称，爱丽丝可以验证预先指定的交易是真实的，并且在她将此策略应用于其名称之前，她能够不受特伦特的影响。这些策略以脚本语言指定，其执行水平与标准签名一样。

Namecoin 并不意味着注册服务机构会消失。在 Namecoin，“注册服务机构”可能非常像特伦特这样。但 Namecoin 确实意味着，注册服务机构伤害其客户的能力比在 DNS 中要小很多，无论是意外伤害还是恶意伤害。最后这可能导致注册服务机构需要的安全预算降低。

像特伦特这样的服务目前在 Namecoin 还没有，但我希望能看到这样的服务。再举一个使用案例，近期的 DDOS 攻击已经开始针对 DNS 基础设施，例如，对 Brian Krebs 的攻击。一些人已经建议，Namecoin 也许能成为有用的防御措施。目前我不清楚 Namecoin 能在多大程度上抵御 DDOS 攻击。

但比特币网络一直在经受压力测试，在过去几年基本上是 DOS 攻击尝试。这些压力测试是由营利性公司进行的，它们具有让比特币网络看起来无力抵抗这类攻击的财务动机。而比

特币丝毫未受影响。Namecoin 也会这样吗？或者，攻击者是否有与比特币压力测试者类似的资源？这很难说。但我认为这是一个有趣的使用案例。我希望将来能有更多这方面的研究。

但为了实现这种确定性，我们需要进行一些权衡。例如，Namecoin 交易是不可逆的。因此，如果一个名称被转让给新的所有者，那么之前的所有者如果没有新所有者的签名，是无法要回去的。这意味着 Namecoin 名称更容易受恶意软件的恶意接管。在这方面，名称所有者的人为错误也可能是一个问题。

一些解决方法包括将私钥保存在完全隔绝的机器上，或者可能将多重或二元认证策略分配给名称，如前所述。这实际上并不全是坏事。我听说安全专家评论说，比特币之所以受到欢迎，其中一个最大的公共优势之一是人们终于开始认真对待终端安全了。由于比特币越来越成熟，我认为终端安全性很可能会得到实质性改善。所以，将来的问题可能会少一些。

另一个权衡是，Namecoin 没有一个非确定性的人来确定哪个名称注册是有效的。所以它有安全方面的好处，而且更多能抵抗政治问题。但这也意味着，如果某人注册了一个侵犯某个商标的名称，就不能轻易地禁用这个名称注册了。你需要与注册商标的人进行协商。

而这正是商标侵权的定义。确定是否发生侵权需要人类来判断，而 Namecoin 明确地设计为不由人类运营。

解决这个问题的是方法，用户可以选择在 Namecoin 客户端和用户的 Web 浏览器之间的某个地方被屏蔽的已知商标侵权名称列表。例如，用于桥接 Namecoin 到 DNS 申请的软件可能支持这一功能作为选项。目前已经有类似这样的基础设施了。PhishTank 就是一个例子。

一个警告是，想要查看侵犯商标的名称的用户可能会故意禁用该屏蔽。但由于商标法的目的就是避免消费者混淆，这可能不是很大的问题。这样做的用户可能已经知道他们在做什么。另一个警告是，有人可能会购买侵权名称，仅用于将其出售给合法商标所有人。但由于注册名称需要花钱，某一个人是难以抢注大量名称的，这与 DNS 名称需要花钱，从而减少了抢注一样。

另一个权衡是隐私。由于整套 Namecoin 交易是公开的，任何人都可以查看交易。通过交易图分析，可以相当容易地了解两个交易是否是是由同一个人完成的。而这也影响了比特币。那么这意味着，如果你为了不同的目的注册两个 Namecoin 名称，那么公开记录可能会显示这两个名称是同一个人注册的。

如果你为其他人购买 Namecoin，他们可能也能看到你注册的名称。一个解决方法是，以不会留下公开记录的支付方式购买 Namecoin。也就是说，如果你重视隐私的话，就不应该用比特币购买 Namecoin。你还应该为你购买的每个名称使用单独

的公钥和私钥对，让它们在交易图表中无法关联。银行转帐可能是不会留下公开记录的购买 Namecoin 的良好方式。此外，有人还在做一些实验，目的是让比特币之类的货币具有更好的隐私，如 Monero 和 Zcash，你可以使用它们购买 Namecoin，然后获取名称。它们有自身的缺点，但对一些用户来说，它们可能是值得的。

总体来说，Namecoin 的参考实施的隐私性很差，难以阻止公众了解你的所有名称都有共同的所有权。我们希望在这方面进行改进，因为这事关重大。

最后一个权衡是 Namecoin 的仅可追加性质的安全性。Namecoin 的所有安全属性都可加密验证，并有一个主要例外，即 Namecoin 名称操作的排序保护并不具有加密安全性。它只具有经济安全性，也就是说，如果要重新排序这些名称操作，需要花一大笔钱。要倒回的时间越久，要花的钱就越多。Namecoin 通常假定，在名称操作发生后大约两个小时内，排序是不可变的。但这并没有通过加密方式得到保证。这具有概率性和经济性，所以它要弱得多。

那么这如何用于实际攻击？那么，回到注册名称之时，如果你可以重新排序交易，那么你就可以在合法注册之前进行一次注册操作，然后窃取名称。

你也可以重新排序名称的续期操作，使其在到期后发生，这会强迫该名称到期，让您可以自己注册。而在现实中，这些都还没有在 Namecoin 发生过。但如果 Namecoin 的使用率提高，会有更多的人尝试这样做。

比特币也有同样的问题。但由于比特币的经济比 Namecoin 大得多，比特币对攻击的防范更强一些。目前有很多积极的研究正在尝试解决次级区块链安全性不如比特币的问题。这一部分是因为如果解决了这个问题，那么比特币的大量改进，包括由资金非常雄厚的公司推动的改进，部署起来要容易得多。所以我们正在非常密切地关注这个研究领域。希望很快会有进展。

我刚刚所说的恶意软件、商标和隐私的任何解决方案都不如 DNS 使用的对策那么简单。而寻找更简洁的解决方案是一个公开的研究问题。也就是说，对于许多现实的使用案例，这些解决方案可能就足够了。

好的。那么发展到什么阶段了？遗憾的是，Namecoin 目前还非常难安装，尤其是你希望 TLS 支持能够运作的话。这主要是由于安装流程还不是非常自动化。我们刚刚从荷兰经济部预算中获得 NLNet 基金会和 Internet Hardening Fund（互联网硬化基金）的资助。这笔资金将用于改善 Namecoin 用作 TLS 公钥基础设施的可用性和应用程序支持。而最终的目标就是 Namecoin 与计算机的名称解析系统和主要的 Web 浏览器的

TLS 实施的集成将可以一步安装。例如，如果你使用的是 Windows，就运行 .exe 安装程序。如果你使用的是 Debian，就运行 .deb 套件。

这笔资金也将用于改进名称所有者的U X，并进行可扩展性和性能改进。这项工作目前主要是我、雨果 • 兰道、布兰登 • 罗伯茨和约瑟夫 • 毕什在做。

我们也在与 Tor 项目积极合作。Tor 的用户群具有不太适合 DNS 的特定安全性要求。他们目前正在使用对人类没有意义的 .ONION，，而且当他们的 Onion 服务 v3 升级推出时，情况会更糟，就像我刚才所说的那样。而问题是，人类在心理上通常不会检查折叠的 onion 地址，这意味着现在外面的诈骗者正在创建现有 .ONION 地址的部分原象来模拟它们。而 Tor 是尽早采纳 Namecoin 的一个很好的选择。由于所有其他可用的选项根本不符合 Tor 的安全要求，所以它们可能会接受 Namecoin 目前的权衡机制状态，而隐私问题可能除外。我是与 Tor 项目开展外展的负责人之一。

最后一个发展领域是后端，我们有一个即将到来的 hardfork，如果你不熟悉区块链术语的话，这是一个完全颠覆向后兼容的升级。这是有必要的，因为比特币对其系统进行了一些升级，我们如果不打破向后兼容，就无法采纳这些升级，而我们希望紧跟比特币。

我们还在考虑其他几个升级，例如让使用期限更加易用，设置不存在的证据，这样您就可以轻松地证明名称是否不存在，从而让名称点节点删除旧数据以获得更好的可扩展性。哈希仍将被保留，所以删除的数据仍然可以被证明，并且还允许使用比特币或者 Monero 或 Zcash 购买 Namecoin，没有任何对手方风险。这些工作大部分是 Daniel Kraft 在做。

谢谢你们邀请我。大家有什么问题吗，我很乐意回答你们的问题。

戴维 • 康纳德： 好的。谢谢你，杰里米。我们有几分钟的问答时间，大家有问题请提出来。好的，史蒂夫。

史蒂夫 • 克罗克： 演讲非常精彩。非常感谢。

杰里米 • 兰特： 谢谢。

史蒂夫 • 克罗克： 我注意到了保护等级以及哪些方面会出错。我所理解的是，无论做出了什么变更，大家都能知道，这就是强大的保护。那么，比如说，根区变更，如果我们采纳根区变更，如果 — 如

果有人改变了根区中的什么东西，大家就会知道。这是一种保护等级，但一些相关方感兴趣的一个其他问题是，我如何防止其他人对我的顶级域采取不良行动，避免发生这种事情。这其中的根源可能是 M of N 与一种可能性相结合，也就是正常人 — 通常会做出变更的人，他的密钥将可以运作，而与之配合的其他密钥可能会被用于超控或类似的其他事情。但我不是 100% 确定可能会发生这种情况。

杰里米 • 兰特： 是的。是的，你当然可以将 Namecoin 用于防止恶意攻击发生。诸如多重签名之类的方法，也就是 M of N 签名，这绝对有益于这一点。同样，我给出的二元认证策略的例子，也可用于这方面。

所以我认为这里有多个使用案例。一个使用案例是确保确实发生的任何恶意事件为公众所知，而且不能从存储器中擦除。但你绝对是正确的，尽量让攻击从一开始就难以发生非常重要。是的，Namecoin 能够实现这一点。由于 — 由于 Namecoin 系统最初是为 — 为拥有标准域名的最终用户设计的，那么有一个想法是，如果你担心你的注册服务机构会以某种方式损害你的名称，他们可能会偶然允许其他人更新名称，通过 Namecoin，如果你愿意的话，你可以成为你自己的注册服务机构。所以你

不需要依赖第三方，除非 — 除非你希望依赖他们获得额外的保护，例如通过多重签名。

史蒂夫 • 克罗克： 有几种情况可能需要第三方干预，首先是分配名称，恢复丢失的密钥，预防流氓行为或对其做出反应等等。所以我在构想系统变化时有一些问题，我们没有适用于这类交易的渠道，并且当然，一旦你那样做，就可以曝光，你可能会获得异常运营商的流氓行为，这关系到如何在其中寻找一个适合度。

杰里米 • 兰特： 好的。是的。那么 —

史蒂夫 • 克罗克： 噢，还有一件事。

杰里米 • 兰特： 请讲。

史蒂夫 • 克罗克： 我们所担心的流氓运营商根本不担心他们会被发现。

杰里米 • 兰特： 是的，我绝对相信这一点。是的，是的，在人们纠正发生的恶意行为的能力与合法用户相信人们无法损害其名称的能力之间，绝对会有一些权衡。这是一种基本的权衡。没有很好的 — 没有一种好的方法能够同时获得这两种保护。因此，Namecoin 可能无法很快完全替代 DNS。事实上，我猜测，相比于 Namecoin，会有很多用户因为这个原因而更喜欢 DNS。也就是说 — 我认为还有很大的用户群希望 — Namecoin 所做的权衡以及他们愿意忍受的 — 忍受的风险，大家知道，如果有人盗窃了他们的私钥，那么就完了。但是，对于如何很好地保护你的私钥，让风险可以忽略不计，这绝对是一个开放的研究问题。是的，这是一个开放的研究问题。

史蒂夫 • 克罗克： 我简单说两句。我对目前的技术的解读是，偷窃私钥是可以忽略的。我的意思是，你把它放在一堆硬件中，如果你猛拉 — 但是其中的权衡是，你的风险会高得多，如果你的私钥被毁坏或丢失，那么你就失去了控制。所以这是需要恢复的行动。

杰里米 • 兰特： 是的。所以如果你不担心恶意方获得你的密钥，但你认为你可以确保 — 但你主要担心你的密钥会被意外毁坏。所以你有一个备份密钥。你可以，比如说，你可以设置一个多重签名策略，1 of N。那么你可以有 N 个备份 — 抱歉，N 减 1 个备份。N1 是

指你可以使用主密钥做一切事情，你也可以申请一个时间日志，使备份密钥只能在主密钥被毁坏时用于恢复名称，然后，比如说，六个月过去了。这还不足以让名称过期，但比如说，如果有人尝试恶意使用其中一个备份密钥，那么除非你已经丢失了主要密钥，否则他们就无法使用备份密钥。所以说，这是个相当灵活的系统。但是的，在某些时候，你依赖于一些密钥不会丢失。

戴维 • 康纳德： 好的。我们还有几分钟问答时间。阿莎。

阿莎 • 合美嘉妮： 好的，谢谢，戴维。感谢你的演讲。我不得不说，我有四分之三的部分没怎么听明白，我想讲一下我的一些简单的理解，想看看我理解的对不对。所以，一种防止攻击的方法是 — 你的域名不会 — 比如说，不会被某个政府或者注册服务机构影响，DNS 在你自己的电脑里生效，数字电话簿在你自己的电脑里。

杰里米 • 兰特： 好的。

阿莎 • 合美嘉妮： 然后比特币在某种程度上可以确保世界上的每台电脑都有同样的数字电话簿或相同的 DNS，这种说法对吗？

杰里米 • 兰特： 是的。是的，总结得非常好。是的。

阿莎 • 合美嘉妮： 好的，太好了。噢。好的。我想回到你的幻灯片中之前提到的 .BIT 话题。现在这是指所有 .BIT 网站，对吗？

杰里米 • 兰特： 是的。是的。Namecoin 目前正在使用 .BIT 顶级域，因此，如果你安装了 Namecoin 软件，它将拦截任何以 .BIT 结尾的任何 DNS 请求，它将会 - 它将会使用 Namecoin 进行查找，而不是 DNS。

阿莎 • 合美嘉妮： 好的。我有两个问题。你说 .BIT 没有在 ICANN 注册。这是一个要求吗？必须这样才能运作吗？

杰里米 • 兰特： 从技术层面上来讲，并不是一定要这样才能运作。我的意思是，即使它没有在 ICANN 注册，也能运作。大家担心的是，假设将来 ICANN 要将 .BIT 顶级域授予其他人，那么系统应该如何运作就不明确了。已经安装了 Namecoin 软件的用户，正如目

前所写的，将使用这种查询功能来访问 Namecoin 网站，但没有安装软件的人会访问 ICANN 授权 .BIT 的任何网站。而尝试访问其他网站的人无法这样做。说白了会有域名空间冲突的风险。所以我们非常希望尝试对它进行正式注册，这样就不会有任何风险，大家知道，将来有人可能会尝试从 ICANN 购买 .BIT，并导致问题。

阿莎 • 合美嘉妮： 好的。这真的很有帮助。非常感谢。

杰里米 • 兰特： 谢谢。

戴维 • 康纳德： 好的。卡韦赫。

卡韦赫 • 兰杰巴尔： 谢谢杰里米的演讲。我有个小问题，因为据我所知，你们并没有把这个提交给 IETF，除了在特殊用途注册管理机构的 .BIT 上进行过一些讨论之外。是有意这样的吗，还是说你们正在计划把它提交给 IETF？

杰里米 • 兰特： 这是一个很好的问题。Namecoin 成立于 2011 年，随便说一下，那时候我还没有参与 Namecoin，最初的作者并不知道特殊用途名称注册管理机构的存在。他们只是推测，好的，我们只希望 ICANN 不会 — 不会将 .BIT 授权给其他人，当然，这不是一个非常明智的决定，但他们不知道 — 他们不知道还有其他选择。

最近，当三个项目 Tor、I2P 和 Ganu.NET 尝试通过特殊用途名称注册管理机构注册其顶级域时，我们听说了它，我们说，噢，这听起来也很适合我们，然后我们联系了互联网草案的作者，他们把我们加到了互联网草案中。遗憾的是，由于政治原因，老实说，我并不适合来讲这个，这份互联网草案被无限期地搁置了。新的互联网草案确实获得通过了，并且成为了 RFC，只添加了 .ONION，也就是 Tor.。所以，三个其他项目，GanuNET、I2P 和 Namecoin 正在等待进展。但是的，我们 — 我们确实积极参与了，也许我们并没有彻底地参与。但一旦我们发现应该跟进的流程，我们已经尽最大努力跟进了。

卡韦赫 • 兰杰巴尔： 非常感谢。

杰里米 • 兰特： 谢谢。

戴维 • 康纳德： 沃伦和丹尼尔 — 实际上沃伦和你讲完之后，就没有其他人了。因为我们要开始下一轮演讲了。沃伦。

沃伦 • 库马里： 我担心的一件事情是，你们对域名的所有权都与公钥 — 抱歉，私钥密切相关，你们有很多有趣的事可以做，例如 M of N 等等，因为用户很难理解这么多。

杰里米 • 兰特： 是的，你说的没错。

沃伦 • 库马里： 就拿比特币来说，我可以有我自己的私人钱包，而且我可以自己记录我的所有东西，但这对于大多数人来说太复杂了，所以他们使用公共的在线钱包，然后被耍了。你们有没有做一些工作来让用户更容易理解他们正在做什么，并让各种材料保持本地化？

杰里米 • 兰特： 这项工作一直在进行中。大部分的工作都是由比特币那帮人，而不是我们完成的，因为他们比我们的资源要多得多。你可能会发现 Bitcoin 世界的产品 GreenAddress 很有趣 — 非常有趣。基本而言，它看起来 — 它是一个比特币钱包，你可以将它作

为手机应用程序进行安装，或者作为浏览器扩展，诸如此类。但它在下面有二元认证。除非你真的需要恢复你的密钥，大家知道，当二元认证服务崩溃时，你真的不需要担心你自己的密钥管理，诸如此类。它尽可能做到简单易用。所以我们非常希望看到 GreenAddress 之类的系统也能和 Namecoin 一起使用。

戴维 • 康纳德： 好的。丹尼尔。

丹尼尔 • 达戴勒： 我有几个问题。首先，你一开始说当前 DNS 系统的非确定性方式是一个问题，但这在多大程度上是一个问题？大家知道，一旦你通过注册服务机构和注册管理机构注册了你的名称，那么它必然是确定性的。是不是名称解析器、缓存，大家知道，它的运作方式和协议数据库交易类似。那么你们正在尝试解决哪一部分的确定性问题？是政策本身还是解析？这是我的第一个问题。

与这个相关的是性能问题。我的意思是，如今的系统本身具有非常好的性能，因为每秒有数百万次解析，而系统使用区块链或内部的追加日志、IP 分类帐，它们是 — 通常它们必须携带整个域名空间来证明使用加密密钥的东西，那么它是如何运作的？我是说，考虑到性能的限制以及仅可追加日志的限制。

杰里米 • 兰特： 好的。非常好的问题。对于非确定性问题，我这几天举出的例子是，如果最初注册了 bit.ly URL 缩短服务，注册它的人可能并没有想到会有这样的看法，噢，.LY 域名将来可能要被伊斯兰国家控制了。那么现在有一个非常真实的风险，ISIS 可能会最终对其进行控制，大家知道，如果 — 如果他们夺取了那个域名，会怎么样？

此外，域名注册服务机构有时候确实会犯错误。现在已经比过去少很多了，但在 DNS 早期，域名注册服务机构曾被诱使将域名转让给没有获得适当授权的其他人，例如，通过发送伪造的传真等等。

我不认为这成为平均情况的风险非常大，但仍然有很大的出错的风险，所以我认为有必要研究一些更具确定性的东西。

对于可扩展性，你说的非常正确，一般来说，区块链和仅可追加数据的结构的可扩展性比 DNS 之类的东西要差很多，是的，你说的非常正确。老实说，目前还不是很清楚 Namecoin 之类的东西能达到多大程度的可扩展性。在昨天我参加的一个小组讨论会上，大家在问答环节中对此进行了一些相当有趣的交流。但它会比现在更大一些。我认为它可以处理 Tor 的 .ONION 服务的大部分用户，而不会有任何麻烦，这仍然是非常有益的。它现在是否会完全取代 DNS？绝对不会。它在遥远的未来是否会完全取代 DNS？这很难说。有可能会，也有可能不会。

戴维 • 康纳德： 好的。谢谢。我想我们已经晚了几分钟了，下一位演讲者是 Farsight Security 的保罗 • 维克西，他要讲的是回应策略区。

保罗，开始吧。

保罗 • 维克西： 谢谢，戴维。那么，总体来说，既然我们在讨论向 DNS 或命名系统添加几层巫术，因为它没有按我们预期的方式运作，我也想提出自己的质疑。

那么，我想指出的是，尽管 ICANN 已经公开宣称，各位首席执行官在各种时间都公开宣称：“我们不是互联网的警察”，这几乎总是为了回应希望能够更轻易地关闭的人，因为在某个地方会有一些域名指向一些资源，对某些人造成伤害，大家知道，前互联网时代的假设是，任何东西都有主人，如果这些东西被用来伤害你，你可以去 — 你可以指出是谁伤害了你，让他们被逮捕，被起诉，或者至少让他们收到你的投诉，然后采取相应行动。

所以，互联网这个东西 — 我不知道 — 一个责任清洗服务，你不断要求关闭一些东西，因为它们伤害了你，最后没有人承认自己是它们的主人，每个人都说：“对不起，我不知道你可以找谁把它关掉，但我没法帮你。”对于因互联网上发生的事情而受伤的人来说，这是非常令人沮丧的。

大家知道，你可以抱怨天气，也可以出去自己做点事。

下一张幻灯片。

那么，我右边的每个人都知道了这些内容，我左边的每个人可能都需要补习一下，为了乔治 • 萨多夫斯基，我还是讲一下这一点吧。

[笑声]

保罗 • 维克西： 域名系统数据流有三层。

最底层是根解析器。这就是你所有的智能手机、笔记本电脑、每个虚拟机、每个 M。构成 DNS 查询的几乎所有东西都是一个根解析器。它要与递归服务器交流，坦白说，这并不是一个很好的名字。我们需要为此设立一个更好的营销部门。

但是请大家不要介意我们正在讨论什么类型的递归，就把它当作空白单词好了。它能够回答你的问题，包括负面的答案 — 没有答案，名称错误，或者没有数据等等。

它使用左边的缓冲来做这件事，所以有一些储存空间。它通常不是图标中显示的磁盘储存，但不管怎么说，它会记住最近的答案，所以如果有很多人问同一件事，你就不必一而再地在互联网中提取答案。

如果有人问你的内容不在你的缓存中，那么你就需要这样做了。你需要上到最顶层，也就是 ICANN 所在的层级。ICANN 的世界是认证服务器。根名称服务器、TLD 服务器、有效的 TLD 服务器、注册服务机构、注册服务机构、注册人，都是认证空间。

从协议角度来看，认证服务器是内容从外面进入域名系统的地方。所以一旦它进入域名系统，你可以使用 DNS 协议提取它，但在可以提取之前，必须先导入。通常从某个文本文件或数据库或某个软件导入。认证机构的工作就是从外部导入 DNS 内容。

那么 ICANN 会议上的这份演示稿的不寻常之处是，我们不会谈论认证服务器或决定创建什么名称或者应该由谁运营什么的策略。大家知道，这是 — 通常来说，过去我经常会提到这些东西，我们花费大量的时间来讨论认证服务器问题以及与之相关的政策，当然，钱都在这些地方，但不同寻常的是，我们现在要讨论的是中层。

原因是，受到以互联网为媒介的伤害的人真的希望能够做点什么，但结果是你不能阻止想要伤害你的人注册域名并放置内容 — 将内容与那些会伤害你的域名相关联。我们需要一个远端解决方案。想象一下，你在互联网的一端，他们在另一端，你需要一个远端解决方案，通过它来阻止，比如说，商标

侵权、知识产权侵权、虐待儿童的材料等等。你会发现各种各样有害的东西，您希望能够从远端阻止它们进入互联网，但你不能，因为互联网发挥的是责任清洗服务的功能。所以，我们已经发展为，不是出于选择而是出于必要，一个近端的解决方案，既然我无法阻止它被创建，而且不能将其可靠地关闭，那么我要让我观察互联网域名系统的角度与伤害我的任何东西的不存在性相兼容。

在这一点上，我们做得非常成功。我们在 2011 年开始这个项目。我们已经修改了三次协议，所以现在是第 4 版协议。目前我们正在对当前的协议进行标准化，之后我们会将关于协议的变更控制移交给 IETF，但目前 IETF 在这方面做的工作还非常少。

这真的类似于一种私人团队工作，而不是像 Namecoin 系统这样的开源项目，所以你们中的有些人为此贡献了想法和功能，但不是通过 IETF 做的，因为我们认为你们很聪明，并且很在意你们发表的意见。

所以我们现在所做的是让外部的观察和分析能够用于制定政策，而这个政策之后将管理响应，我稍后会谈到“Z”，但我想要说，缓存不受此影响。

你可以想象一下，一个政策说：“天啊，有一个新的域名生成算法僵尸网络，它正在创建所有这些名称。它和 Conficker 之类

的差不多。而且我们想确保如果有人查找这些名字之一，他们不会得到答案，因为答案可能会告诉我的一个机器人或我的网络上的一些被感染的客户端如何实现一个命令和在别人的网络上控制服务器，我不 — 我必须拦截那个地方。我选择在 DNS 拦截它。”

那么，你可能要说：“好吧，那么这些名称，僵尸网络今天要使用的这些可计算的名称是被禁止的。”这可能就是你制定的政策。

但明天，明天就不是这样了，对吧？明天又会有一套不同的名称集。这些域生成算法僵尸网络在计算要使用的名称时使用了日期。你不想一直阻止名称。这真的会 — 会加剧冲突的可能性，确实存在冲突，即使这些名称 —

像 Conficker 这样的域名生成算法僵尸网络会产生非常难看的名字，但是它会与我认为难看的真正的非恶意名称相冲突。所以你想要删除这些。

我们没有在缓存中放入政策。实际上，我们将事实放入缓存。

所以响应政策机制只会影响根解析器将要看到的东西。它不会影响储存的内容，也不会影响从认证机构提取的内容。

我之前说过我要讲一下“Z”。“Z”是一个区，反映了这样一个事实，递归服务器已经存在于互联网。有 2500 万个，大部分

不应该存在。它们是小小的愚蠢的有线调制调节器，不应该运行那个服务，但却在运行。其中大概 200 万个是有意的。所以大概有 200 万个递归服务器比较重要。有开放的 DNS 以及谷歌和它的 8.8.8.8。有很多递归服务器很重要。它们是 — 我看看 — 我想怎么说？

我们希望能够使用外部数据来控制这些服务器的策略，并且很多这些服务器都深深存在于现有网络的内部，疯狂地在防火墙后面，所以它们无法到达外部，外部也不能访问它们。

将你的递归域名服务器放在防火墙后面被认为是良好的安全卫生做法，这样它们就不会被线下的人用作 DDOS 放大器。

但我们发现，其中很多人可以在线下谈论 DNS 协议，所以我们决定是否可以偷偷实行政策，让 DNS 数据通过 TCP 端口 53 提取，就像提取其他 DNS 数据一样，这有可能会奏效，而且这些递归服务器将能够订阅一个策略源。因此，我们开始尝试将响应策略塞到 DNS 区的形式中。

所以，这将是你有史以来看到的最丑陋的 DNS 区。它全是不应该自然发生的模式，非常不自然，看起来非常可怕。

你可以对它的可怕感到自豪，因为这些可怕之处本身就是一个艺术项目。

工作流程是，有人在那里，在右上角进行观察和分析。他们断定：“好吧，一个新的僵尸网络，新的 DGA，今天不应该解析的新的名称集”，或者它可能是一个新的 IP 地址块，你知道它正在被垃圾邮件发送人利用，也许他们有一个非法广播电台，正在宣传一些不属于他们的 BGP 空间，我们真的希望确保，会产生该非法空间内 A 记录或 AAAA 记录的任何答案在今天无法解析。

所以，你将所有观察和分析结果转储到响应策略区中，然后通过递归服务器以正常的区域传输方式订阅。

现在我想指出，这是一种自愿行为。递归服务器运营商希望这样。这不是 SOPA。这不是上游的人对你做的，你没法避免。

此外，如果你的递归服务器订阅了其中某个东西，而你不喜欢它，那么你可以切换到 8.8.8.8，这具有很大的自愿性，即使是对于根解析器而言。整个方法尽管可以用于尝试影响审查制度，但实际上并没有。必须将它看作是一种增值，或者它不会被递归服务器运营商或根解析器运营商利用。

所以我也想讲一下这一点。

那么，数字是什么呢？某个给定的递归服务器可能会使用我所知道的一些软件，或者 PowerDNS 或者 — 还有第四个，运行 BIND 或者 Unbound。有四个独立的实施不会相互分享源代码，它们都能正确地互操作。在 IETF 世界，如果你有多个可

互操作的实施，那么你可以开始认为，也许协议文件已经足够完整了。所以，有了四个，我认为已经齐了。

有数千个递归服务器订阅一个或多个响应策略区。有十几个安全提供商在这个论坛中发布其观察和分析结果。罗德 • 拉斯穆森代表其中一个，或者最近这样做了。

但有一个网站 dnsrpz.info 列出了所有这些实施，所有这些发布者，并且包含了规范的指针。社群这样做是为了在近端保护自己，防止受到我们无法阻止的远端引入的问题的影响。这种方式奏效了。十分奏效。

我们 — 我的公司现在提供一种采用这种区格式的安全策略，受到了欢迎。我想罗德在他最近的公司中在这方面取得了一些成功。所以这对于安全行业来说是有好处的，因为它为我们的东西提供了更多的客户，对于那些试图保护自己的人来说也是一个很好的选择，因为它为他们提供了一个新的网络阻塞点和一个非常开放的标准，对于他们想要订阅哪些安全策略，他们可以有一个多供应商解决方案。

最后，这也是一个企业解决方案。尽管我提到罗德和我都是出售这些策略的，但有一点也很常见，比如说，一家银行会有一个他们今天不想解决的事情的清单。在没有这种技术的情况下，他们在域名空间中的任何一点创建空区域，他们希望用一点点涂改液，让人们无法看到。如果你要做 600 万个，而且每

天都要变动其中的一半，那么你的域名服务器配置就有大量变动，非常糟糕。然而，对于响应策略区之类的东西，你不用更改你的域名服务器。你只要更改响应策略。这是非常简便的操作。

所以，不可避免的是，安装这个的人首先做的是创建一个由自己的安全部门维护的本地响应策略区域，以便当他们意识到这些威胁时 — 还是一个观察和分析 — 他们可以将这些响应策略以一种类似矩阵的方式快速转储到递归域名服务器中，你将它转储到一个地方，然后突然间它就在所有地方同步了，然后企业不再回答某些问题，或者是不再回答会产生特定答案的问题。

其他策略可能是，不回答可能涉及特定域名服务器名称的问题。所以，基本上你可以在不知道问题或答案是什么的情况下对内容投毒；但是你知道它是来自该域名服务器名称还是处于特定范围的域名服务器 I.P. 地址，然后情况就变糟了。有很多节点。戴维 • 康纳德曾经告诉我，我们现在有足够的绳子，任何想要吊死自己的人现在都可以做到这一点。

我想我要提的最后一件事，也是我们经常做的，就是我们说“我想说谎”，然后假装确实存在的某个东西不存在。换句话说，这是假的，合成的 NXDOMAIN 信号。NXDOMAIN 是 DNS 中的返回代码值，表明你提的问题涉及的是不存在的东西。但

是，这不是你唯一可以做的事，因为很多人不想这样做。他们会创建一个所谓的围墙花园，比如说，你正在查找一个 Conficker 名称，一个有域名生成算法的 Conficker 僵尸网络。你真正想要的可能是在用户的显示屏上弹出一个窗口，说：“嗨，你感染了 Conficker”。而且，你可以这样做 — 而不是使用合成 NXDOMAIN 来回答，您可以使用合成别名回答，你要查找的东西的规范名称为 walledgarden.example.com。一些由企业自身运行的 Web 服务器会告诉人们：“嗨，你可能被感染了，应该立即联系 IT 部门。”除了撒谎某个东西是否存在之外，还有很多其他事情可以做。

我想，在进入问答环节之前，最后一个话题就是我们在撒谎。这些是谎言。也就是说 — 认证机构是你认为恶意的人拥有的，你不想知道真相。然后你决定自己骗自己，因为这样可以让你的网络和资产对特定的威胁做出响应。当你说谎时，其中一个被破坏的东西就是 DNSSEC。而 DNSSEC 对于世界经济的未来非常重要。我们必须有它，不仅仅是为了 DANE，而且是为了渠道中各种阶段的所有其他有 DNSSEC 意识的应用程序。而这对它造成了破坏。如果你这样运行，而数据本身由认证机构签署，那么我们的代码就会忽略它。我们的代码不会对经 DNSSEC 签署的名称实行策略。这让坏人们能够非常容易地避开这些，他们只打开 DNSSEC。

但是根解析器也会要求 DNSSEC。目前 DNSSEC 的普遍性还不足以避免这些发生。但在某个时间点，这可能会成为一个问题。而且我完全希望，在我们发布当前的规范和将更改控制权交给 IETF 之后，几乎会立即出现一个完全像这样的新协议，除了它对 DNSSEC 更明智一点之外。所以这是一个目前还没有影响我们的已知的弱点。但我真的希望它能影响我们，因为如果它影响到我们，就意味着 DNSSEC 变得普遍了，而这正是我们需要的。这就是我准备的发言，现在进入问答环节。戴维，我们还有几分钟？

戴维 • 康纳德： 我们有大概五到七分钟的时间向保罗提问。谁想开始提问？

没有问题要问保罗吗？好的。就从我开始吧。

[笑声]

那么，保罗，我认为 RPZ 的其中一个影响是，它有点加强了很多新 gTLD 在普遍适用性方面的问题。首先，我这样说对吗？其次，有没有什么办法可以处理？

保罗 • 维克西： 我有个儿子在域名行业工作过一段时间。当 .ENTERPRISES 推出时，他注册了 VIXIE.ENTERPRISES，我认为这个名字非常可爱，因为我在他出生之前有过一家咨询公司。

然后他继续尝试使用这个名称，发现 .ENTERPRISES 并不是其中一种形式，比如说，联合航空公司希望你关联你的帐户。幸运的是，我认识联合航空公司的人，所以能够解决这个问题。但他遇到各种问题。所以我非常理解这些新的通用 TLD 非常难以使用，因为很多人认为，大家知道，可能是 .COM、.NET、.ORG、.INFO 或者一堆国家代码。如果不是这样，那一定是语法错误。所以我明白这一点。但这并不是来自 RPZ，并且我没有听说过这个问题与 RPZ 有关。

戴维 • 康纳德： 好的。你指出 RPZ 与 DNSSEC 不能配合。我之前认为，RPZ 可以与 DNSSEC 配合，因为如果一个区域被签署，则返回的响应可以被验证。验证之后，返回到根解析器的答案可以根据 RPZ 的适当指示进行修改。

保罗 • 维克西： 基本上是这样。如果根没有要求 DNSSEC，当然可以这样。如果你没有把 D.O. 设置为等于 1，那么你刚才说的就会发生。我们会提取数据。如果可能的话，我们会进行验证。我们会把它放入缓存。然后，当我们尝试坚定最初问题的答案时，我们会说，等一下，有策略。根并没有请求 DNSSEC，所以我们要 — 我们会瞎编故事，因为如果根无法判断我们在撒谎，那么我们

就会撒谎。但是如果根要求 DNS 记录，并且有 DNS 记录，我们就不会应用策略。

戴维 • 康纳德： 乔治？

乔治 • 萨多夫斯基： 谢谢保罗的补习。我差不多准备好接受测试了。

所以我想，与这个问题更相关的是提供策略所依据的信息的人。

谈谈这里的存活时间考虑因素。你们多久播放一次？你们提供给用户的变更的频率如何？你们如何知道存活时间是多少？

保罗 • 维克西： 好的。不管你们信不信，我很高兴你能提出这个问题。连接是实时的。所以 — 如果你做了一个变更，由于这是一个正常的 DNS 区域，所以会有一个通知，会有增量区域传输，并且几乎会立即更新。所以，在你改变主意的时候，你说，天哪，我十分钟前喜欢这个策略，但现在我不喜欢它了，你可以改变主意，这将立即反映在你的用户群中。我们不能破坏任何新事物，这一点非常重要。为此，如果 — 我们不希望系统里有任何过期数据。我给大家举个例子。

我的公司出售一项新观察的域名服务。这是因为我们已经发现，互联网每秒创建 2 1/2 个新的授权点，其中大约一半将在 24 小时内消失。1/6 会在十分钟内消失。变动率非常高。这些东西目的就是为了惹恼一些人，而且在许多情况下会几乎立刻被关闭，或者被 SpamHaus 之类的人列入黑名单。但这不意味着所有的新事物都是坏的，但确实意味着新事物在统计学上有变坏的可能性。

我还记得过去的那些好时期，你要求一个 .COM 名称，如果是在星期二之后，你会在星期五得到它，我不介意新的域名没有这么好。ICANN 及其生态系统已经经过发展，将其缩短到 30 秒，没有我所担心的非恶意使用案例。

这意味着我们必须向我们的 RPZ 订阅者每秒发送一次更新，说：“这是我们发现的新域名。顺便说一下，我们现在删除了超过十分钟的旧域名，因为你们只需要新的，而按照你们的定义，它已经过了十分钟，不是新的了。”我们有不同的定义。

每秒发送一次更新的网络能够在数千个合成客户或数十个实际客户之间同步响应策略。这样可以奏效。流动性非常大。没有什么是过期的。

戴维 • 康纳德： 沃伦？

沃伦 • 库马里： 我认为这更像是个意见，而不是问题。我曾经为一些域名运行自己的域名服务器，然后收到大量垃圾邮件，让我非常恼火，所以我把它们关闭了。

然后我开始订阅一群不同的人的 RPZ 订阅源，我已经把它们全部重新打开了，因为通过 RPZ，我几乎没有垃圾邮件要处理，对吧？通过 RPZ，我收到了一群人的垃圾邮件订阅源。它只是处理一些事情，现在它又重新奏效了。这是...

保罗 • 维克西： 谢谢你的意见。我来说几句。

除非 DNS 发挥作用，否则你在互联网上将无法完成工作。我知道有很多对等协议，所以当 DNS 不工作时，并非所有 BitTorrent 的人都能发现。但是对于我们其他人来说，如果 DNS 不起作用，那么可以到达哪些地址是不重要的，因为我们不会输入 I.P. 地址。我们当然不会输入 IPv6 地址。

现在，这种属性对坏人们也奏效。如果 DNS 不工作，不仅仅是好人们无法完成工作。如果坏人不在 DNS 中，就没法访问他们。

对于我来说，你提到了垃圾邮件。对于我来说，这意味着，这意味着电子邮件垃圾邮件，因为我出生时。

我的邮件比较严格，它是 Postfix，它的构造是在页眉中的每个名称、信封中的每个名称，以及正文中的每个名称中进行 DNS 查询。如果其中任何一个失败，我会拒绝邮件，这意味着利用这个阻塞点来说这些名字应该是不存在的，如果它们恰好存在，那么就撒谎说它们不存在，这会导致您的基础设施中发生所有各种各样的其他故障。你要为之做好准备。当你没有收到垃圾邮件时，它们可能会有点令人惊讶。事实上，你所说的是整个工作的次要目的。

戴维 • 康纳德： 好的。谢谢保罗所讲的 RPZ，现在有请保罗 • 胡特斯。

保罗 • 胡特斯： 谢谢。

现在麦克风在我这里，我就讲一会。我得说，保罗 • 维克西和约翰 • 吉尔摩是地球上最难以向他们发送电子邮件的两个人，因为他们主要部署了防御或缺乏防御机制。

那么，鉴于 —

>> （不在麦克风前。）

保罗 • 胡特斯： 附带损害。

要大规模部署 DNSSEC，这有点麻烦。人们需要将 DS 记录放入其父区，这是一个非常困难的过程，它涉及太多的人，最重要的人在注册人那里工作，然而他并不知道什么。他只是购买了一项服务和一个域名，其他什么也不知道。他只是想让它运作，有一个域名运营商为他运行一切，所以他们甚至连 DNSSEC 是什么都不知道，他们不知道如何启用它，即使他们的 DNS 运营商告诉他们要做什么，但他们真的很难做到这一点。

所以，在各种非常大的托管服务提供商中，有很多域名基本上已经被签署，但没有 DS 授权记录，所以即使他们确保了自己的安全，也只是一个小小的孤岛，因为 DS 记录没有进入父区，因为没有办法做到这一点。

所以，这个问题需要一个解决方案。

而 IETF 首先避开了解决这个问题，但在某个时候，它变得了一个非常大的问题，所以他们回来了，他们 — 这是令人费解的。我要关上笔记本电脑了。

所以，他们需要做的两件事情 — 在上周刚刚发布的 RFC-8078 中，这已经完成了 — 他们需要以某种方式让 DNS 运营商向注册管理机构发出信号，告诉他们这个域名现在有 DS 记录，请发布此 DS 记录。

然后 DS 运营商还需要的就是能够说“我的客户都跑了，我的客户不想继续使用 DNSSEC。”当不再需要 DNSSEC 时，我们需要通过某种方式让注册管理机构再次删除记录。

RFC 基本上允许这样做。它所做的是创建了 — 它使用了记录时间 CDS，基本上与 DS 的记录类型完全一致，只是它是在客户端侧发布的，也就是说在客户端区本身。

所以一旦它发布之后，你就能通过某种方式联系你的注册管理机构，说：“嗨，我已经发布了这个 CDS 记录。你可以看一下吗，如果你认为可以的话，请将它作为 DS 记录发布在你的父区。”

所以这是新记录的功能。

抱歉。记录并不做这个工作。它的用途是新的。

你可以通过各种方式联系你的注册管理机构，这将在其他草案中说明。目前还有另一个草案，例如，使用一个 Restful 界面，使用 HTTP 来传达信息，但人们也可以提出其他机制。然后，特殊禁用记录是全部是零的 CDS 记录，这其实是说“请禁用这个，我们不想要任何东西。”

这张幻灯片上有一个错别字。应该有第四个零，这也是上次修订草案中的一个问题，但是我们赶在 RFC 发布之前发现了它，但显然我没有更新我的幻灯片。

所以说，这套系统是有用的。因为现在还有新的 EPP 扩展，注册管理机构，一旦他们接受了来自 DNS 运营商的这种超出限制的更新，他们就可以将其发回他们的注册服务机构，让他们也知道这个记录已被更新，不会通过传统的 EPP 流进来。

目前这正在部署中或者 — 一些 TLD 正处于部署阶段，所以很快这意味着将有成千上万的 DNSSEC 签署的域名被授权，所以这应该是 DNSSEC 部署的一大进展，是的，我们希望这能取得圆满成功。

戴维 • 康纳德： 好的。还有问题要问保罗吗？

好的，利曼。

拉斯 • 约翰 • 利曼： 我是拉斯 • 利曼。我想澄清一下。这不是欧拉夫 • 科尔克曼提议的 CDS 记录？还是在 IETF 中提出的？

保罗 • 胡特斯： 好的。这是欧拉夫 • 科尔克曼的 RFC，是的。

拉斯 • 约翰 • 利曼： 好的。谢谢。这有点强调了 DNS 运营商与注册管理机构之间缺乏正式关系，我认为，这很好。

保罗 • 胡特斯： 我不是故意要提到它的。

戴维 • 康纳德： 帕特里克？

帕特里克 • 弗斯特朗姆： 你们有没有看看 —

在你们的左边。

[笑声]

帕特里克 • 弗斯特朗姆： 正常情况下会发生什么 — 请看幻灯片。

在正常情况下，DNSSEC 交易将通过注册服务机构进行，所以注册服务机构具有完整的最后责任，以确保关于注册人的所有内容都完整，包括密钥 — 关键材料。

这种情况下，密钥的更新是从 DNS 运营商到注册管理机构的，不经过注册服务机构，对吧？

保罗 • 胡特斯： 对。

帕特里克 • 弗斯特朗姆： 你是说这是通过 EPP 中的事件触发的，对吗？

所以注册服务机构应该使用 pull 命令来提取关于新密钥材料的信息。

是这样的吗？

我担心的是，如果注册服务机构突然没有对该区域的完整观点，这个问题 — 可能会影响到与注册管理机构有关的注册服务机构的责任。

保罗 • 胡特斯： 是的，没错。是的。但我认为，有一个新的 EPP 扩展让注册管理机构能够使用 push 命令，所以这不像注册服务机构那样需要 pull 命令。

帕特里克 • 弗斯特朗姆： 没错。你可以通过扩展那样做。但 — 在正常 EPP 设计中，完整的设计是让注册服务机构更新注册管理机构，而不是另一个方向。

保罗 • 胡特斯： 对。

帕特里克 • 弗斯特朗姆： 好的。所以，这是另一件事情，注册管理机构在注册服务机构中规定了状态机器的变化，而我们有非常非常少的这些，这是另一件事情，对吗？

保罗 • 胡特斯： 好的。但注册服务机构可能也支持同样的机制，让他们的注册人与他们交流。

所以对于那些愿意实施所有 DNSSEC 要求的人来说，他们不需要这种通融方法，因此也不需要创建状态机器。只要注册服务机构与 DNS 运营商建立了良好的合作关系，可以相互交流。由于注册服务机构无法与 DNS 运营商交流，那么问题就仍然存在，他们无法获得这些信息，除非使用这种机制。

帕特里克 • 弗斯特朗姆： 可以使用 DNS 查询与你交流，对吗？

不管怎么样，对于透明度，我在查看这份文档时，我建议这份文档应该 — 应该标准化这种出色的 CDS 记录，无论是注册管理机构还是注册服务机构在拉动它。

保罗 • 胡特斯： 注册服务机构在哪里发布它？你是说，如果注册服务机构通过 EPP 发送它？

帕特里克 • 弗斯特朗姆： 不是。发布 — 注册服务机构从 DNS 运营商那里提取新的 DS，并使用 EPP 将它推送到注册管理机构。

保罗 • 胡特斯： 即使没有这份草案，他们也已经可以这样做了。

戴维 • 康纳德： 那么 —

帕特里克 • 弗斯特朗姆： 这个问题我们私下再谈。是的。我之前已经在 IETF 电子邮件清单中解释过一次了，可能不需要再解释一次。

戴维 • 康纳德： 好的。丹和沃伦。

丹 • 约克： 那么，我想谢谢保罗介绍这一点，我认为关键点是，也许是，对于不想深入了解其中一些细节的 ICANN 董事会成员和其他听众而言，他们能意识到，正在进行一部分工作是，为 DNSSEC 的工作方式提供更好的自动化，因为当我们看到 DNS 运营商或其他人试图大规模部署 DNSSEC 时，确定的一个重大障碍之一就是获取这些信息，这些 DS 记录，一直到注册管理机构。

因此，这是现在注册管理机构可使用的机制之一，他们可以选择这些机制帮助信息发布的自动化，从而更好地实现这一点，最终使 DNS 更安全。

所以，这是 — 这是真正的关键点，这是一个新的机制，现在已经可以使用，所以注册管理机构可以查看它，作为实现这一点的一种方式。

对于帕特里克的观点，注册服务机构也可以查看它。

戴维 • 康纳德： 沃伦？

沃伦 • 库马里： 我之所以要打断帕特里克，是因为我认为大家的意见各不相同。

我认为，拉斯，你说过草案最初是由欧拉夫撰写的。是的，欧拉夫是原创者。欧拉夫和我自己。是的。

初始文档并不能自动阻止人们停止发布这些记录。你需要经过注册管理机构或注册服务机构，我认为这就是帕特里克所说的。由于帕特里克提出了同样的担忧，我们特意省略了“你可以绕过你的注册服务机构”。这是以旧草案为基础的，并增加了新的功能。可能我也误解了你的 —

帕特里克 • 弗斯特朗姆： 我想要做的是将技术功能单独拿出来讲，也就是 DNS 运营商示意这是新的密钥材料的能力，来自关于注册人、注册服务机构和注册管理机构之间关系的可能的政策影响。这个讨论完全不同，可能在某个 TLD 中非常乱。

戴维 • 康纳德： 我很快地回应一下。是的。

>> 帕特里克，需要解决的基本问题是指出谁是注册人，什么是与它进行交流的工具。我们的注册管理机构数量有限，所以方便作为交流的起点，但是如果我们能够以某种方式进入 RDAP 或其他协议，为愿意与我们交流的实体找到工具，最好是注册管理机构或分销商，甚至是分销商的分销商，这是目前没人能找到的东西。

戴维 • 康纳德： 德米特里？

德米特里 • 柯曼约克： 大家好。我想快速讲一下为什么注册管理机构框是双重的。我觉得是打错字了。第二，我想对帕特里克 • 弗斯特朗姆表示赞同，是的，EPP 模型 — 我，顺便说一下，代表 TLD、ccTLD 之

一。我们运行 EPP。是在乌克兰。我认为状态分裂的模式很不好。我还觉得拉动模式很不好，并且不能扩大规模。但是 — 是的，EPP 支持 DS 更新，但我最大的问题是，我们正在尝试分离 DNS — 抱歉，NS 记录和 DS 记录管理。这样不好。因为变更 DNS 运营商可能同时涉及 DS 记录变更和 DNS 记录变更。有点奇怪的是，DS 更新应该是（听不清）这份草案，并且不监管 DNS 记录。

所以我想说，如果你能回到绘图板，看看注册服务机构的整个分离情况，例如，关于实体名称、地址和材料的数据更新，而不是技术数据。是的，失去第三方技术运营商是一个好主意，但这是错误的解决方案，加上 DNS 运营商之间缺乏合同关系，一个或两个，注册管理机构是错误的解决方案，这不是解决这个问题的方法，也这不是让互联网更安全的方法。

所以，这是个不错的尝试，但我 —

保罗 • 胡特斯： 那么 — 我想快速回应一下，然后交给保罗 • 维克西讲。

IETF 已经对触发器和计时器进行了很长时间的讨论，我们再来重复一次。

这是注册管理机构可以决定使用的选项，如果有些注册管理机构根据合同不能使用它，或者不想使用它，也没关系，但对于

目前不能将 DS 记录推送到正确地方的很多人来说，这是一个有用的选择方案。

德米特里 • 柯曼约克： 是的，对。有很多问题。我认为我们现在不应该讨论这个。最好在 IETF 环境中讨论。谢谢。

保罗 • 胡特斯： 好的。

戴维 • 康纳德： 保罗？

保罗 • 维克西： 我想强调那一点。NomCom 经过很大的努力才聘用到愿意服务于董事会的优秀人士，他们并不一定像早在 ICANN 存在之前就已用过多年互联网的那些人一样具有很强的技术性。我们必须明智地使用他们的时间，并尊重他们的时间，所以请你们在讨论时让乔治 • 萨多夫斯基也能听懂。

[笑声]

戴维 • 康纳德： 接下来，大家还有没有什么其他要说的。

大家知道，在某种程度上，这是一次重新组织 TEG 运营方式的努力。我们在会前向董事会成员提供了一两页的简报，想知道这是否有用，或者我们是否应该继续尝试发展 TEG，让它对董事会成员更有用。

你可以现在说，也可以给我发电子邮件，或者在马上要举行的鸡尾酒会上找我。大巴大概 15 分钟后离开。好的，我宣布本次 TEG 会议到此结束，感谢大家的参加。

[鼓掌]

[会议记录结束]