COPENHAGEN – Reunião conjunta: Diretoria da ICANN e TEG (Grupo de especialistas técnicos)
Quarta-feira, 15 de março de 2017 – 17h às 18h30
ICANN58 | Copenhagen, Dinamarca

STEVE CONTE: Caso alguém esteja procurando o grupo de aceitação universal, informo que ele foi transferido desta sala para a B5.1. Não que não queiramos sua presença aqui, mas se o que vocês estão procurando é a aceitação universal, e não a sessão do grupo de especialistas técnicos, a sala correta é a B5.1. E quero jogar batalha naval agora.

DAVID CONRAD: O que... ah, uau. A festa pode começar. Jonne está aqui.

>> (Fora do microfone.)

DAVID CONRAD: Na verdade, ainda estamos fazendo alguns malabarismos logísticos agora. O Steve e a Lousewies disseram que estão chegando, ele devem estar aqui em breve. Estamos tentando fazer malabarismos com alguns slides agora.

Observação: O conteúdo deste documento é produto resultante da transcrição de um arquivo de áudio para um arquivo de texto. Ainda levando em conta que a transcrição é fiel ao áudio na sua maior proporção, em alguns casos pode estar incompleta ou inexata por falta de fidelidade do áudio, bem como pode ter sido corrigida gramaticalmente para melhorar a qualidade e compreensão do texto. Esta transcrição é proporcionada como material adicional ao arquivo de áudio, mas não deve ser considerada como registro official.

>> (Fora do microfone.)

DAVID CONRAD: Sim, realmente podemos começar com algumas apresentações, se vocês quiserem. Para fins de contexto, será a diretoria contra os especialistas técnicos, luta livre na gaiola. Certo. Talvez não.

Esta é a reunião... não sei qual o número, do grupo de especialistas técnicos. Esta reunião foi definida para que os especialistas técnicos possam fazer contribuições à diretoria. Não fornecemos pareceres, fazemos contribuições. Ela é... originalmente, era uma sessão fechada, mas decidimos abri-la para receber a participação de todos os interessados em coisas de nerds.

Vamos ver. Aparentemente, foi perguntado se o RSSAC e o SSAC foram convidados para esta reunião ou não. Bem, em primeiro lugar, é uma reunião aberta e, em segundo lugar, pode ter havido alguma confusão, porque nós... em que reunião foi isso? Na de Marrakesh? Não lembro em qual reunião, mas tivemos de adiar... tivemos de cancelar o TEG para fazer coisas relacionadas com a transição, então, em vez de realizar a reunião do TEG, decidimos fazer um coquetel do TEG com a diretoria. Ainda, para que a coisa ficasse um pouco mais divertida, também

convidamos o RSSAC e o SSAC, então foi um coquetel da diretoria com o TEG, o SSAC e o RSSAC que agora virou uma espécie de semitradição. E é isso, os membros do TEG e os membros da diretoria estão convidados a participar do coquetel no Ruby esta noite, por volta das 19h.

>> 19h.

DAVID CONRAD: 19h, com um ônibus que vai sair às 18h45 da frente do...

Na verdade, você tem um microfone.

>> Isso, após a sessão, às 18h45, vamos ter um transporte de bom tamanho que vai sair do Bella Center, entrada oeste, que fica aqui ao lado.

Às 18h45, embarquem nessa conosco. Obrigado.

DAVID CONRAD: E o Steve chegou, então, e também o Jonne, a festa pode começar.

>> (Fora do microfone.)

DAVID CONRAD: Exatamente. Gostaria de dizer algo?

STEVE CROCKER: Claro. Peço desculpas por ter chegado atrasado. Fico muito feliz por ver tanta gente aqui. Isto é fantástico. O David está no comando.

[Risos]

DAVID CONRAD: Certo. Bem, vamos começar com as apresentações.

Marc, por favor. Seu nome, empresa, cor favorita. Não sei.

MARC BLANCHET: Marc Blanchet.

JAY DALEY: Meu nome é Jay Daley, .NZ.

DANIEL DARDAILLER: Daniel Dardailler, W3C.

LITO IBARRA: Lito Ibarra, da diretoria da ICANN.

KAVEH RANJBAR: Kaveh Ranjbar, técnico e da diretoria da ICANN.

LARS JOHAN-LIMAN: Lars Johan-Liman, diretor de operações do servidor raiz da Netnod.

GEORGE SADOWSKY: George Sadowsky, da diretoria da ICANN.

RINALIA ABDUL RAHIM: Rinalia Abdul Rahim, da diretoria da ICANN.

PATRIK FALTSTROM: Patrik Faltstrom, presidente do SSAC.

ASHWIN RANGAN: Ashwin Rangan, da equipe da ICANN.

CHERINE CHALABY: Cherine Chalaby, da diretoria da ICANN.

MARKUS KUMMER: Markus Kummer, da diretoria da ICANN.

TERRY MANDERSON: Terry Manderson, da equipe da ICANN, diretor de engenharia do DNS e diretor da área de Internet na IETF.

ALAIN DURAND: Alain Durand, da equipe da ICANN, pesquisa da OCTO.

ASHA HEMRAJANI: Asha Hemrajani, da diretoria da ICANN.

PAUL VIXIE: Paul Vixie, da Farsight Security, convidado.

JEREMY RAND: Jeremy Rand, do projeto Namecoin.

PAUL WOUTERS: Paul Wouters, contato da IETF.

STEVE CROCKER: Steve Crocker, da diretoria da ICANN.

DAVID CONRAD: David Conrad, da organização ICANN.

STEVE CONTE: Steve Conte, da equipe da ICANN org.

CATHY PETERSEN: Cathy Petersen, da equipe da ICANN org.

WENDY PROFIT: Wendy Profit, da equipe da ICANN org.

JONNE SOININEN: Jonne Soininen, contato da IETF com a diretoria da ICANN.

DAN YORK: Dan York, da Internet Society com enfoque nas DNSSEC.

SUZANNE WOOLF: Suzanne Woolf, do SSAC, do RSSAC, agitadora aleatória.

WARREN KUMARI: Warren Kumari, contato da IETF.

ED LEWIS: Ed Lewis, da ICANN org, pesquisa da OCTO.

ROY ARENDS: Roy Arends, da ICANN, pesquisa da OCTO.

MATT LARSON: Matt Larson, também da ICANN, pesquisa da OCTO.

FRANCISCO DA SILVA: Francisco da Silva, do ETSI e minha empresa é a Huawei, Suécia.

HOWARD BENN: Howard Benn, também representando o ETSI.

JULIE HAMMER: Julie Hammer, do SSAC.

ROD RASMUSSEN: Rod Rasmussen, do SSAC.

>> (dizendo seu nome), da ITU-T.

ADIEL AKPLOGAN: Adiel Akplogan, da equipe da ICANN, envolvimento técnico.

GREG AARON: Greg Aaron, do SSAC.

MAARTEN BOTTERMAN: Maarten Botterman, da diretoria da ICANN.

JAAP AKKERHUIS: Jaap Akkerhuis, da comissão de especialistas do SSAC e RSSAC.

LOUSEWIES VAN DER LAAN: Peço desculpas por ter chegado atrasada. Lousewies Van der Laan, da diretoria da ICANN.

JOHN CRAIN: Eu estava me escondendo lá no fundo e achei melhor vir para a frente. John Crain, da organização ICANN, diretor de SSR.

DAVID CONRAD: Certo. Muito obrigado.

Bem, a pauta já está na tela. Esta é a sessão de boas-vindas e administrativa.

Apenas para reiterar o que dissemos antes, se alguém estiver procurando a reunião do grupo de gestão de aceitação universal, ela foi transferida para a sala B5.1, que fica neste mesmo corredor. No entanto, todos são bem-vindos aqui. Esta é, obviamente, a luta livre em gaiola entre o grupo de especialistas técnicos e a diretoria.

Prosseguindo, acho que vamos começar com uma apresentação do Jeremy Rand, do projeto Namecoin, que vai falar sobre o Namecoin. Portanto, Jeremy, pode começar.

JEREMY RAND: Olá. Meu nome é Jeremy Rand e sou do projeto Namecoin, então vamos começar.

Primeiro, uma revelação importante. Sou um dos desenvolvedores mais ativos do Namecoin e não conheço nenhum desenvolvedor do projeto que possa discordar de qualquer coisa nesta apresentação. No entanto, não posso falar em nome de todos os desenvolvedores sobre todas as coisas. Somos um projeto de código aberto que não tem uma estrutura organizacional clara, é importante que todos saibam disso.

Esta apresentação foi preparada em colaboração com o Hugo Landau.

Bem, a motivação subjacente do Namecoin é que os seres humanos se comportam de maneira não determinística e, por extensão, qualquer sistema executado por seres humanos se comportará de maneira não determinística.

Em particular, mesmo que um sistema tenha regras básicas que devem ser invioláveis, as regras básicas que forem aplicadas por seres humanos serão aplicadas de maneira inconsistente.

Por exemplo, as leis da constituição dos EUA estabelecem regras básicas que afirmam que a tortura e a vigilância em massa estão fora de questão. Infelizmente, essas regras básicas são aplicadas por seres humanos e, portanto, como todos sabemos, essas regras não são aplicadas de maneira determinística, como seria esperado.

E o comportamento humano no futuro distante é ainda mais não determinístico.

Por exemplo, prever os resultados de uma eleição torna-se mais difícil quanto mais longe no futuro elas se realizarem e, portanto, prever o ambiente político de um país fica cada vez mais difícil quanto mais tempo avançarmos no futuro.

E o DNS é, em grande parte, operado por seres humanos. Isso apresenta um risco, porque as pessoas envolvidas na operação do DNS podem ter um comportamento não determinístico.

É possível que seu registrador cometa um erro e permita que outra pessoa altere seus registros, ou é possível que o governo, que tem a propriedade de seu ccTLD, seja derrubado daqui a dez anos e o novo governo decida que não gosta de seu nome e decida apreendê-lo, ou é possível que a pressão política tenha como resultado que, no futuro, a ICANN implemente uma nova política com a qual você não concorda agora.

Qualquer uma dessas coisas pode acontecer, e isso é preocupante.

Portanto, o Namecoin é um experimento para descobrir se é possível construir algo que seja vagamente semelhante ao DNS, mas com o menor envolvimento humano possível, e criar um sistema semelhante ao DNS que se comporte de maneira mais determinística que o DNS. Temos a esperança de que um sistema assim seja mais confiável e mais seguro contra modos de falha causados por seres humanos, porque o sistema será mais determinístico.

Bem, vejamos alguns sistemas de identificadores existentes para compará-los com o Namecoin.

A nomenclatura manual em um site, coisas como arquivos do host, elas não têm um espaço de nomes global, o que significa que os nomes só têm um significado localmente, mas elas estão protegidas contra seres humanos não determinísticos e têm nomes com significado para os seres humanos, o que é bom.

A nomenclatura hierárquica como o DNS tem um espaço de nomes global, mas não está protegida contra seres humanos não determinísticos. Ela tem nomes com significado para os seres humanos. A facilidade de uso é muito alta, mas é arriscado como raiz de confiança.

O endereçamento de conteúdo, como BitTorrent, onde o nome é o hash, tem um espaço de nomes global e está protegido contra seres humanos não determinísticos, mas não tem nomes com significado para os seres humanos e o conteúdo nunca pode ser alterado.

Uma variante disso é quando o nome é a chave pública. Coisas como os domínios .ONION que a Tor usa. Eles têm um espaço de nome global e estão protegidos contra seres humanos não determinísticos, mas também não têm nomes com significado para os seres humanos. No entanto, o conteúdo pode ser alterado. Esse tipo de sistema é seguro como uma raiz de confiança, mas tem uma facilidade de uso muito baixa. O usuário verá uma URL como a que vocês podem ver na tela ao tentar digitar alguma coisa.

Na verdade, estou mentindo. A Tor está fazendo uma atualização de segurança agora e, quando terminar, os nomes ficarão assim.

[Risos]

JEREMY RAND: Sim. Vocês devem ter notado que nos slides anteriores havia duas marcas de verificação e um X, e esse é o triângulo de

Zooko. Bem, Zooko Wilcox conjeturou que era impossível atingir os três pontos ao mesmo tempo.

Passando para um tópico um pouco diferente, os registros públicos apenas para anexos estão cada vez mais populares para garantir a responsabilidade. O exemplo de maior sucesso disso é a transparência de certificados da Google. Cada certificado usado na rede pública está sendo colocado em um registro apenas para anexos, e os navegadores provavelmente terminarão exigindo que os certificados sejam registrados para serem válidos. E mesmo que você queira manter o controle sobre um sistema, talvez queira que todas as ações sejam publicadas.

A transparência de certificados é um registro apenas para anexos de certificados, mas não é muito adequada para usar com sistemas como o DNS, e o motivo disso é: quem pode gravar no registro? Qualquer um. Mas apenas os certificados de autoridades reconhecidas podem ser gravados. Isso é bom para garantir que os registros não sejam atacados por spam com dados inúteis, mas uma lista manual de entidades confiáveis é, de certa forma, inconveniente.

O Namecoin é um registro apenas para anexos de registros de nomes e atualizações. No entanto, ao contrário da transparência de certificados, o Namecoin é implementado

usando uma blockchain, portanto, ele pode impedir spam impondo um custo econômico à gravação de dados. Esse custo é pequeno, mas muito eficaz. Ele desincentiva os malfeitores de ocuparem nomes em massa sem depender de uma lista manual de entidades confiáveis.

O Namecoin tem um espaço de nomes global, está protegido contra seres humanos não determinísticos e tem nomes com significado para os seres humanos, portanto, é uma solução para o triângulo de Zooko. O Namecoin significa que pode ser operado um registro apenas para anexos da nomenclatura como um fórum aberto, aprimorando sua utilidade. A responsabilidade e a transparência podem, assim, ser transformadas em um bem público verificável por meio de criptografia. E, independentemente do sistema de regras que o Namecoin usar para nomes, sua natureza enquanto registro apenas para anexos significa que, se um malfeitor fizer alguma coisa, sempre se saberá.

Como exercício de raciocínio, imaginem uma zona raiz responsável. A responsabilidade pode satisfazer às partes normalmente desconfiadas de que não está acontecendo nada incompleto.

Como exemplo hipotético, manter a zona raiz como um registro apenas para anexos para dar uma satisfação aos países de todo

o mundo que o controle dos EUA não está sofrendo abuso, nem mesmo no nível intergovernamental.

Os servidores raiz poderiam alimentar-se diretamente do registro. Uma zona raiz mantida como um registro apenas de anexos poderia dar u7ma satisfação aos países de que, por exemplo, os respectivos ccTLDs não sofrerão interferência por motivos políticos, de maneira mais ou menos análoga ao monitoramento sísmico usado pelos países para verificar uns aos outros conforme o tratado contra testes nucleares que garante a paz. Confie, mas verifique. E, para sermos claros, não estou recomendando que seja implementada esta ideia em particular no DNS, mas é um estudo de caso hipotético interessante.

Mudando um pouco de assunto, um problema relacionado é a infraestrutura de chave pública de TLS. O sistema de autoridades de certificados usado hoje é problemático, mesmo com a transparência de certificados. O problema subjacente aqui é que há seres humanos demais envolvidos, os quais podem cometer erros. As DNSSEC e a DANE, que armazenam dados de TLS no DNS, em vez de ter autoridades de certificados que os verifiquem, poderiam melhorar a situação. Infelizmente, também há questões políticas envolvidas. Algumas pessoas ficam nervosas com a possibilidade de abuso da raiz do DNS ou dos operadores de TLDs.

E, novamente, o problema aqui é que a raiz do DNS e os operadores de TLDs também têm seres humanos envolvidos. Portanto, isso não resolve totalmente o problema do envolvimento de seres humanos. O Namecoin poderia proporcionar as vantagens das DNSSEC e da DANE para esta finalidade sem incluir os problemas políticos.

Bem, não esperamos que a maioria dos programas de software ou mesmo das bibliotecas de resolução de nomes conheçam diretamente o Namecoin. Em vez disso, esperamos que o software de ponte entre o Namecoin e o DNS seja instalado localmente, traduzindo as consultas ao DNS em consultas ao Namecoin e convertendo as respostas do Namecoin novamente para o DNS.

O Namecoin usa o domínio de primeiro nível .BIT, que atualmente não está registrado na ICANN ou na IETF. Gostaríamos de encontrar uma forma viável de resolver isso. Sabemos que é um problema. Por exemplo, poderíamos usar os registros de nomes de uso especial, como .ONION foi usado pela Tor.

Nossa referência de limite, chamada NCDNS, atua como um servidor oficial do DNS para o domínio de primeiro nível .BIT executado no anfitrião local. Os usuários das DNSSEC geram um tempo de instalação, e nós intencionalmente tentamos manter

a especificação do nome de domínio do Namecoin facilmente mapeável para o DNS, de modo que o software de ponte possa ser facilmente utilizado.

Se, hipoteticamente, alguém quisesse usar isso, poderia dizer ao servidor recursivo do DNS, por exemplo, o Unbound, para usar NCDNS como confiável para .BIT e fornecer a chave pública de DNSSEC do NCDNS. Em teoria, tudo deveria funcionar. São apenas algumas linhas em unbound.com.

Na prática, há alguns recursos do DNS que não são amplamente compatíveis. Por exemplo, a DANE para TLS. Portanto, temos de fazer algumas personalizações estranhas de multiplicação para fazer esse negócio funcionar. Uma vez, eu tentei conferir quantas camadas diferentes de bruxarias loucas estávamos usando para fazer a DANE do Namecoin funcionar corretamente em navegadores que não são compatíveis com a DANE para TLS. E parei de contar na quinta camada de bruxarias.

Então, em que casos reais de uso o comportamento determinístico do Namecoin pode nos ajudar? Bem, digamos que você esteja tentando comprar ou vender um nome. No DNS, a compra ou venda de um nome normalmente envolve algum risco de contraparte, e talvez você tenha que confiar em um agente depositário para atenuar esse risco.

No Namecoin, o comprador e o vendedor podem construir conjuntamente uma transação que pague atomicamente o vendedor e transfira o nome para o comprador. Isso elimina o risco de contraparte sem exigir os serviços de um agente depositário.

E isso é ótimo, mas e se o comprador e o vendedor não quiserem nem mesmo conversar para definir a transação atômica? Você pode comprar ou vender ofertas. E o fluxo de trabalho funciona mais ou menos assim. A Alice pode criar uma oferta de venda. Eu quero vender o nome de domínio exemplo.bit por 100 Namecoins. A Alice assina a oferta de venda com sua chave privada, o que prova que ela é a proprietária de exemplo.bit e está disposta a transferir o domínio em troca de 100 Namecoins. A Alice pode publicar essa oferta de venda assinada em um fórum ou pastebin, ou algo parecido.

O Bob vê a oferta e quer comprar exemplo.bit. O Bob pode preencher a oferta, assinando-a com uma chave privada que tenha 100 Namecoins. E esta oferta será então uma transação válida do Namecoin. O Bob pode transmitir para a rede do Namecoin sem entrar em contato com a Alice novamente.

A Alice recebe o pagamento. O Bob recebe o domínio. E esta transação é atômica. Não há risco de contraparte e não é necessário usar um agente depositário. Isso funciona tanto para

ofertas de compra como para ofertas de venda. O protocolo do Namecoin já é compatível com esse tipo de uso, e esperamos contar com ferramentas amigáveis para o usuário em breve.

Além disso, outro exemplo de uso é que um nome normalmente é de propriedade de uma única chave privada, mas também é possível que a propriedade seja de várias chaves privadas, sendo que M de N chaves devem estar presentes para emitir uma atualização. Isso pode ser uma proteção útil contra uma chave única comprometida. Por exemplo, uma diretoria pode ter uma chave privada e a atualização do nome pode exigir uma maioria qualificada da diretoria. Novamente, o protocolo do Namecoin já é compatível com esse tipo de uso, e esperamos contar com ferramentas amigáveis para o usuário em breve.

O Namecoin também pode permitir a elaboração de políticas de atualização muito flexíveis, as quais podem ser usadas para personalizar coisas com base na segurança e nas necessidades de experiência do cliente do proprietário de um nome. Por exemplo, digamos que a Alice seja proprietária de um nome, mas queira limitar o risco de sua chave privada ser roubada sem correr muitos riscos de contraparte. Ela pode elaborar uma política que seja mais ou menos assim: A Alice pode contratar o Trent para executar um serviço de autenticação de dois fatores. Em seguida, Alice pode atualizar seu nome com dados arbitrários, se o Trent assinar suas atualizações. E o Trent

promete só fazer isso após verificar por meio da autenticação de dois fatores.

Além disso, o Trent pode pré-assinar transações específicas para determinados eventos nos quais a Alice possa querer fazer algo depois sem a autorização de Trent. Por exemplo, talvez a Alice queira poder revogar seu registro de TLSA. Assim, se o seu servidor da Web for comprometido, ela pode revogar o certificado facilmente. Ou talvez a Alice fique preocupada por que o Trent possa desaparecer, sair do negócio ou perder sua chave privada. Portanto, essas políticas podem ser especificadas com base em restrições personalizáveis. O Trent não pode transferir nem atualizar o nome da Alice sem a assinatura dela, e a Alice pode verificar se as transações pré-assinadas são autênticas e se ela está protegida contra o Trent antes de aplicar esta política a seu nome. E essas políticas são especificadas em uma linguagem de script e são aplicadas no mesmo nível que as assinaturas convencionais.

O Namecoin não significa que os registradores vão deixar de existir. No Namecoin, os “registradores” talvez sejam parecidos com o Trent. Mas o Namecoin significa que os registradores têm muito menos capacidade de prejudicar seus clientes do que no DNS, seja um prejuízo acidental ou malicioso. E isso poderia acabar resultando em uma redução necessária do orçamento de segurança dos registradores.

Os serviços como os que o Trent oferece ainda não existem no Namecoin, mas eu gostaria de ver um serviço desse tipo. Em outro exemplo de uso, digamos que a infraestrutura do DNS tenha sofrido ataques de DDOS recentes, por exemplo, o ataque contra Brian Krebs. Algumas pessoas sugeriram que o Namecoin poderia ser uma defesa útil. Bem, para mim, não está claro como o Namecoin enfrentaria um ataque de DDOS.

No entanto, a rede do Bitcoin foi submetida a testes de resistência, que são basicamente tentativas de ataque de DOS, nos últimos anos. Os testes de resistência foram realizados por empresas sem fins lucrativos que tinham um incentivo financeiro para tentar fazer a rede do Bitcoin parecer fraca contra esses ataques. E o Bitcoin saiu praticamente ileso. Será que o Namecoin teria o mesmo sucesso? Será que os atacantes teriam recursos semelhantes aos dos que testaram a resistência do Bitcoin? É difícil dizer. Mas acho que é um exemplo interessante. Eu gostaria de ver mais pesquisas sobre isso no futuro.

Para ter esse determinismo, no entanto, precisamos fazer algumas concessões. Por exemplo, as transações do Namecoin são irreversíveis. E, consequentemente, se um nome for transferido para um novo proprietário, o proprietário antigo não poderá obtê-lo novamente sem a assinatura do novo proprietário. Isso significa que os nomes do Namecoin são um

pouco mais vulneráveis a apropriações hostis por malware. E, a propósito, os erros humanos por parte do proprietário do nome também poderiam ser um problema.

Entre as formas de evitar isso, podemos manter suas chaves privadas em uma máquina fisicamente isolada ou talvez atribuir aos nomes políticas de autenticação de dois fatores ou várias assinaturas, como comentei antes. Na verdade, isso não é de todo ruim. Já vi especialistas em segurança comentando que uma das maiores vantagens públicas da popularidade do Bitcoin é que as pessoas finalmente estão levando a segurança de pontos periféricos a sério. À medida que o Bitcoin amadurecer, acho que é provável que a segurança de pontos periféricos aumente consideravelmente. Portanto, talvez isso não seja um problema no futuro.

Outra concessão é que o Namecoin não tem um ser humano não determinístico para determinar quais registros de nomes são válidos. E é por isso que ele tem vantagens de segurança e é mais resistente a questões políticas. No entanto, isso também significa que, se alguém registrar um nome que infrinja uma marca comercial, não haverá um modo fácil de desativar esse registro de nome. Será necessário negociar com a pessoa que registrou o nome.

E isso é basicamente inerente à definição de infração de marca comercial. Para determinar se ocorreu uma infração, é necessário uma intervenção humana, e o Namecoin foi especialmente projetado para não ser operado por seres humanos.

Uma forma de contornar isso seria que os usuários pudessem entrar em uma lista de nomes conhecidos que infringem marcas comerciais, que seriam bloqueados em algum ponto entre o cliente do Namecoin e o navegador da Web do usuário. Por exemplo, o software do DNS que é usado para fazer a ponte entre aplicativos do Namecoin para o DNS poderia oferecer isso como uma opção. Já existe uma infraestrutura para coisas desse tipo. O PhishTank é um exemplo.

Uma advertência é que um usuário que quisesse ver um nome que infringe uma marca comercial poderia desativar intencionalmente o bloqueio. Mas como a finalidade da lei de marcas comerciais é evitar a confusão dos consumidores, é provável que isso não seja um grande problema. O usuário que fizesse isso provavelmente saberia o que está fazendo. Outra advertência é que alguém poderia comprar um nome infrator unicamente para vendê-lo ao respectivo proprietário legítimo. Mas, como o registro de nomes custa dinheiro, é difícil que uma única pessoa se aproprie indevidamente de uma grande quantidade de nomes dessa forma, assim como o fato de o

registro de nomes do DNS custar dinheiro também reduz a apropriação indevida.

Outra concessão é a privacidade. Como o conjunto completo de transações do Namecoin é público, qualquer um pode ver as transações. A análise do gráfico de transações torna relativamente fácil descobrir se duas transações foram feitas pela mesma pessoa. E isso também afeta o Bitcoin. Portanto, o que isso significa é que, se você registrar dois nomes diferentes do Namecoin para finalidades diferentes, provavelmente será público que ambos os nomes foram registrados pela mesma pessoa.

E, se você comprar Namecoins de outra pessoa, ela provavelmente poderá ver os nomes com que você os registrar. Uma forma de contornar isso é comprar Namecoins com um método de pagamento que não deixe registro público. O que significa que você não deveria usar Bitcoins para comprar Namecoins se valoriza sua privacidade. E você também deveria usar pares de chaves públicas e privadas separadas para cada nome que comprar, de modo que eles não possam ser vinculáveis no gráfico de transações. As transferências bancárias poderiam ser uma boa forma de comprar Namecoins sem deixar um registro público. E, além disso, foram feitos experimentos para criar moedas semelhantes ao Bitcoin que são melhores em termos de privacidade, como o Monero e o Zcash,

que poderiam ser usados para comprar Namecoins e obter nomes. Essas moedas também têm suas desvantagens, mas podem ser úteis para alguns usuários.

Em geral, a implementação de referência do Namecoin tem uma privacidade muito fraca e torna difícil impedir que o público saiba que todos os seus nomes têm um proprietário em comum. Queremos fazer melhorias neste sentido, porque é uma questão importante.

A última concessão é a segurança da natureza apenas para anexos do Namecoin. Todas as propriedades de segurança do Namecoin são verificáveis por meio de criptografia, com uma grande exceção: a ordem das operações de nomes do Namecoin não é protegida por criptografia. Em vez disso, ela é protegida apenas economicamente, o que significa que custaria muito dinheiro reordenar as operações de nomes. E quanto mais se retrocede no tempo, mais dinheiro custa. O Namecoin normalmente supõe que a ordem é provavelmente imutável até cerca de duas horas após a ocorrência de uma operação de nome. Mas isso não é garantido por criptografia. É de natureza probabilística e econômica, portanto, muito mais fraco.

Então, como isso poderia ser usado para um ataque prático? Bem, se você pudesse reordenar as transações voltando ao momento em que um nome foi registrado, você poderia colocar

uma operação de registro para esse nome antes do registro legítimo, e assim roubaria o nome.

Você também poderia reordenar as operações de renovação do nome para que ocorressem após o prazo, o que forçaria o nome a perder a validade e permitiria que você o registrasse. Nada disso nunca aconteceu na vida real no Namecoin. Mas, se a adesão ao Namecoin aumentar, mais pessoas poderão tentar fazer isso.

O Bitcoin tem o mesmo problema. Mas, como a economia do Bitcoin é muito maior que a do Namecoin, o Bitcoin ganha muito mais segurança contra ataques. E há muita pesquisa ativa para resolver esse problema de as blockchains secundárias serem menos seguras que no Bitcoin. Em parte, porque muitas melhorias no Bitcoin, inclusive algumas pelas quais estão pressionando empresas muito bem financiadas, serão muito mais fáceis de implementar se esse problema for resolvido. Então, estamos acompanhando bem de perto essa área de pesquisa. E esperamos que haja progresso em breve.

Nenhum dos contornos que acabei de descrever para malware, marcas comerciais e privacidade é tão direto quanto as medidas tomadas no DNS. E encontrar soluções mais elegantes continua sendo um problema de pesquisa aberto. Dito isso, para vários

exemplos de uso do mundo real, esses contornos provavelmente sejam suficientes.

Certo. Então, qual o caminho do desenvolvimento? Bem, infelizmente, o Namecoin agora é realmente difícil de instalar, especialmente quando se quer que a compatibilidade com TLS funcione. E isso acontece principalmente porque ainda não está muito automatizado no processo de instalação. Acabamos de receber um financiamento da NLNet Foundation e do Internet Hardening Fund com verba do ministério da economia dos Países Baixos. Esse financiamento será usado para melhorar a facilidade de uso e a compatibilidade com aplicativos para o uso do Namecoin como infraestrutura de chave pública. E o objetivo final é que a integração do Namecoin com o sistema de resolução de nomes de um computador e com as principais implementações de TLS dos navegadores da Web possa ser instalada em uma única etapa. Assim, por exemplo, se você estiver no Windows, executará um instalador .exe. Se estiver no Debian, executará um pacote .deb.

E esse financiamento também será usado para melhorar a experiência do usuário para proprietários de nomes e para melhorias da capacidade de expansão e do desempenho. Este trabalho está sendo feito principalmente por mim, pelo Hugo Landau, pelo Brandon Roberts e pelo Joseph Bisch.

Também estamos ativamente envolvidos com o projeto Tor. A base de usuários do Tor tem requisitos de segurança específicos que não são muito apropriados para o DNS. Eles estão usando agora o domínio .ONION, que não tem significado para os seres humanos, e isso vai ficar pior quando a atualização do Onion Services v3 for lançada, como mostrei antes. E o problema é que, psicologicamente, os seres humanos normalmente não verificam o endereço onion por extenso, o que significa que, neste momento, há falsificadores soltos por aí criando pré-imagens parciais de endereços .ONION existentes para se fazer passar por eles. E o Tor é um bom candidato para a adoção precoce do Namecoin. Eles provavelmente podem viver com o estado atual das concessões do Namecoin, com a possível exceção dos problemas de privacidade, porque todas as outras opções disponíveis simplesmente não cumprem os requisitos de segurança do Tor. E atualmente sou eu quem lidera o envolvimento com o projeto Tor.

A última área de desenvolvimento está no back-end. Temos um hardfork a caminho. Caso vocês não estejam familiarizados com a terminologia das blockchains, trata-se de uma atualização que quebra totalmente a compatibilidade com versões anteriores. Isso foi necessário porque o Bitcoin lançou algumas atualizações para o sistema deles que não pudemos adotar sem

quebrar a compatibilidade com versões anteriores, e queremos continuar próximos ao Bitcoin.

Também estamos analisando várias outras atualizações, coisas como tornar o período de validade muito mais amigável para o usuário, ter provas de não existência de contato de modo que possa ser facilmente provado se um nome existe ou não, ou permitir que nós de pontos de um nome descartem dados antigos para melhorar a capacidade de expansão. Os hashes ainda seriam mantidos, de modo que os dados descartados ainda poderiam ser comprovados, e também permitir a compra de Namecoins usando Bitcoins, ou talvez Monero ou Zcash, sem nenhum risco de contraparte. A maioria dessas iniciativas está sendo liderada pelo Daniel Kraft.

Bem, obrigado pelo convite. Estou aberto às perguntas.

DAVID CONRAD: Certo. Obrigado, Jeremy. Temos alguns minutos para perguntas, caso alguém queira pedir a palavra. Sim, Steve.

STEVE CROCKER: Bem, foi uma apresentação excelente. Muito obrigado.

JEREMY RAND: Obrigado.

STEVE CROCKER: Eu estava prestando atenção no nível de proteção e no tipo de coisas que podem dar errado. A proteção forte é que as eventuais alterações feitas são conhecidas, no meu entender. O... então, em uma situação de, digamos, alteração da zona raiz, se adotássemos isso... se alguém alterasse alguma coisa na zona raiz, isso seria conhecido. É um nível de proteção, mas um problema diferente no qual algumas partes estão interessadas é como posso impedir uma ação adversa contra meu domínio de primeiro nível, para que ela não possa ser realizada. E talvez as sementes disso estejam nesse M de N combinado com a possibilidade de que a pessoa normal... a pessoa que normalmente faria a alteração, sua chave funcionará e as outras chaves juntas seriam usadas para uma anulação, ou algo parecido. Mas não ficou 100% claro para mim que isso é tudo o que poderia acontecer.

JEREMY RAND: Sim. Então, sim, você pode definitivamente usar o Namecoin para a finalidade de impedir que aconteçam ataques maliciosos. Coisas como o método de várias assinaturas, que é M de N assinaturas, podem realmente ser uma vantagem nesse sentido. Da mesma forma, o exemplo que dei sobre a política de autenticação de dois fatores também pode ser usado para isso.

Então, sim, acho que há vários exemplos de casos aqui, Um exemplo é assegurar que qualquer coisa maliciosa que acontecer seja publicamente conhecida e não possa ser apagada da memória. Mas, sim, você tem toda razão, é importante poder tentar dificultar ao máximo possível a realização de ataques. E, sim, o Namecoin pode ajudar nesse sentido. Como o Namecoin foi originalmente projetado para os usuários finais proprietários de um nome de domínio convencional, uma ideia seria, bem, se você tem medo que seu registrador possa danificar seu nome de alguma forma, que ele possa permitir que outra pessoa o atualize por acidente, com o Namecoin, se você quiser, poderá ser seu próprio registrador. Portanto, você não precisa depender de um terceiro, a menos que queira depender de um para obter mais proteção, como no caso das várias assinaturas.

STEVE CROCKER: Há vários casos nos quais pode ser necessária a intervenção de um terceiro, na alocação do nome em primeiro lugar, na recuperação de chaves caso sejam perdidas, na prevenção ou reação contra comportamentos perigosos etc. Então, tenho dificuldade para imaginar uma variação no sistema que temos que não tenha avenidas para esse tipo de transações e, é claro, assim que você fizer isso, terá a exposição de poder sofrer um

comportamento perigoso por parte do operador excepcional, então, é uma questão de encontrar um meio-termo entre eles.

JEREMY RAND: Certo. Sim. Então...

STEVE CROCKER: Ah, mais uma coisa.

JEREMY RAND: Claro.

STEVE CROCKER: O tipo de operadores perigosos que nos preocupa não estaria nem um pouco preocupado em ser descoberto.

JEREMY RAND: Sim, eu realmente pensaria isso, sim. É, sim... realmente há uma concessão entre a capacidade de um ser humano de corrigir um comportamento malicioso que ocorreu e a capacidade de um usuário legítimo de ser convencido de que um ser humano não poderá causar danos ao seu próprio nome. É, é uma concessão importante. Não existe uma boa maneira de obter ambos os tipos de proteção ao mesmo tempo. O Namecoin, por esse motivo, provavelmente não substituirá o DNS por enquanto. Na

verdade, eu diria que há uma quantidade muito grande de usuários que preferem o DNS em vez do Namecoin, por esse motivo. Dito isso, existe... eu acho que também existe uma quantidade importante de usuários que quer as concessões que o Namecoin faz e está disposta a assumir o risco de que, bem, se alguém roubar sua chave privada, então... fim do jogo. Mas, sim, realmente é um problema de pesquisa aberto sobre a forma de tornar a proteção de suas chaves privadas tão boa que o risco seja desprezível. E, sim, é um problema de pesquisa aberto.

STEVE CROCKER: Uma réplica rápida. O que eu entendo da tecnologia atual é que o roubo de uma chave privada é desprezível. Quero dizer, você a coloca em um conjunto de hardware que, se você apertar... mas a concessão é que há um risco muito maior de perder o controle se a sua chave privada for destruída ou perdida, ou algo assim. Então, essa é a ação que requereria recuperação.

JEREMY RAND: Sim. Bem, se você não tiver medo que uma parte maliciosa obtenha sua chave, mas achar que pode garantir que... mas se sua preocupação principal for que sua chave possa ser destruída por acidente, então, sim. Você pode ter uma chave de reserva disponível. Você poderia, por exemplo, ter uma política de várias assinaturas que fosse 1 de N. Assim, poderia ter N

reservas... desculpe, N menos 1 reservas. N1 significa que você poderia usar a chave principal para tudo e também poderia aplicar um registro de hora, para que as chaves de reserva só pudessem ser usadas para recuperar o nome caso a chave primária fosse destruída e, digamos, decorressem seis meses. O que não é tempo suficiente para que o nome perca a validade, mas possibilita que, digamos, se alguém tentasse usar maliciosamente uma das chaves de reserva, isso só poderia ser feito se você também tivesse perdido a chave primária. Então, sim, é um sistema bastante flexível. Mas, sim, em algum ponto, você deverá confiar que uma quantidade determinada de chaves não será perdida.

DAVID CONRAD: Certo. Temos mais alguns minutos para perguntas. Asha.

ASHA HEMRAJANI: Sim, obrigada, David. Obrigada por essa apresentação. Devo dizer que não entendi talvez três quartos do que você disse, então elaborei uma versão simplificada na minha cabeça e queria ver se entendi certo. Bem, uma forma de prevenir ataques e... bem, em vez de seu nome de domínio estar em risco por parte de, digamos, um governo ou um registrador, o DNS está ativo em seu próprio computador, e a agenda telefônica digital está, de certa forma, em seu próprio computador.

JEREMY RAND: Sim.

ASHA HEMRAJANI: E então o Bitcoin mais ou menos garante que cada computador no mundo tenha a mesma agenda telefônica digital ou o mesmo DNS, é uma descrição aceitável?

JEREMY RAND: Sim. Sim, é um excelente resumo. Sim.

ASHA HEMRAJANI: Certo, ótimo. Ufa. Certo. Bem, então, quero voltar à parte sobre o .BIT que você mencionou antes nos slides. Isso agora diz respeito a todos os sites do domínio .BIT, certo?

JEREMY RAND: Sim. Sim. Então, o Namecoin atualmente está usando o domínio de primeiro nível .BIT e, como consequência, se você tiver o software do Namecoin instalado, ele interceptará as solicitações do DNS para qualquer site que termine com .BIT e os procurará usando o Namecoin, em vez do DNS.

ASHA HEMRAJANI: Certo. Bem, tenho duas perguntas. Você mencionou que o .BIT não está registrado na ICANN. Isso é um requisito? Para que funcione.

JEREMY RAND: Não é um requisito para que funcione em um nível técnico. Quero dizer, isso já funciona agora, mesmo não estando registrado na ICANN. A preocupação é, se, hipoteticamente, a ICANN concedesse no futuro o domínio de primeiro nível .BIT a outro, aí não ficaria claro como o sistema funcionaria. As pessoas que têm o software do Namecoin instalado, e isso está gravado neste momento, acessariam os sites do Namecoin usando essa pesquisa, mas as pessoas que não o têm acessariam qualquer um a quem a ICANN delegasse o domínio .BIT. E as pessoas que tentassem acessar o outro não poderiam fazê-lo. Portanto, há um risco de colisão de espaço de nomes, basicamente. É por isso que realmente gostaríamos que ele fosse registrado oficialmente, para que não haja nenhum risco de que, bem, alguém tente comprar o .BIT da ICANN no futuro e cause problemas.

ASHA HEMRAJANI: Certo. Isso realmente ajuda. Muito obrigado.

JEREMY RAND: Obrigado.

DAVID CONRAD: Certo. Kaveh.

KAVEH RANJBAR: Obrigado, Jeremy, pela apresentação. Tenho uma pergunta rápida, porque, até onde sei, você não levou isso para a IETF além de discutir um pouco sobre o .BIT para o registro de uso especial. Foi uma escolha consciente? Você tem planos de levar isso para a IETF ou não?

JEREMY RAND: Essa é uma boa pergunta. Bem, quando o Namecoin foi fundado, em 2011 – e, a propósito, isso foi antes do meu envolvimento no Namecoin –, os autores originais não tinham ideia de que existia o registro de nomes de uso especial. E eles basicamente pensaram, certo, vamos só esperar que a ICANN não autorize o domínio .BIT a outra pessoa. Obviamente, essa decisão não foi muito sábia, mas eles não sabiam que havia outra opção.

Mais recentemente, quando três projetos – Tor, I2P e Ganu.NET – tentaram registrar seus domínios de primeiro nível por meio do registro de nomes de uso especial, ficamos sabendo e

pensamos, ah, parece uma boa ideia para nós também, e entramos em contato com os autores dessa versão preliminar da Internet e eles nos adicionaram a ela. Infelizmente, por motivos políticos sobre os quais eu, sinceramente, não sou a melhor pessoa para falar, essa versão preliminar da Internet foi colocada em espera indefinidamente. Uma nova versão preliminar da Internet foi aprovada e tornou-se uma RFC que somente adicionou o .ONION, que é do projeto Tor. Assim, os outros três projetos, GanuNET, I2P e Namecoin, ainda estão esperando que haja algum avanço nesse sentido. Mas, sim, nós nos envolvemos ativamente, e talvez não tenhamos sido tão eficientes no envolvimento como deveríamos. Mas, sim, assim que soubemos que havia um processo que deveríamos estar seguindo, tentamos fazê-lo da melhor maneira que pudemos.

KAVEH RANJBAR: Muito obrigado.

JEREMY RAND: Obrigado.

DAVID CONRAD: Warren e Daniel... na verdade, Warren e depois você, e vamos encerrar a fila de inscrições porque... para a próxima apresentação. Warren.

WARREN KUMARI: Bem, uma das coisas que me preocupa é que toda a propriedade do domínio esteja vinculada à chave pública... desculpe, chave privada, e há muitas coisas interessantes que você pode fazer, como M de N etc., mas para os usuários pode ser bem difícil entender tudo isso.

JEREMY RAND: Sim, você está certo.

WARREN KUMARI: Tipo, com o Bitcoin, eu posso ter minha própria carteira privada e posso manter o controle, eu mesmo, sobre todas as minhas coisas, no entanto, isso é muito complexo para a maioria das pessoas, então elas usam carteiras on-line públicas que são de propriedade de terceiros. Há algum trabalho em andamento para tentar tornar isso muito mais simples para que os usuários possam entender o que exatamente eles estão fazendo com isso e para que as coisas continuem no nível local?

JEREMY RAND: Sim, há trabalho sendo feito nesse sentido. A maior parte desse trabalho está sendo feita pelo pessoal do Bitcoin, e não por nós, simplesmente porque eles têm muito mais recursos que nós.

Talvez você ache o produto GreenAddress, no mundo do Bitcoin, bem interessante. Basicamente, ele parece... é uma carteira do Bitcoin que você pode instalar como aplicativo móvel ou como extensão do navegador, coisas desse tipo. Mas ele tem a autenticação de dois fatores escondida. E, a menos que você realmente precise recuperar suas chaves, se esse serviço de autenticação de dois fatores for desativado, você realmente não deverá preocupar-se com o gerenciamento, coisas assim. Ele tenta tornar isso o mais amigável possível para o usuário. E, sim... realmente gostaríamos de ver sistemas como o GreenAddress sendo usados com o Namecoin também.

DAVID CONRAD: Certo. Daniel.

DANIEL DARDAILLER: Algumas perguntas. Primeiro, você começou dizendo que a abordagem não determinística do sistema do DNS atual é um problema, mas em que medida isso é um problema depois que um nome é registrado, depois de passar pelo registrador e pelo registro, aí deve ser determinístico. É o resolvedor de nomes, o cache, enfim, e funciona como uma transação de banco de dados de protocolo. Então, que parte do problema determinístico vocês estão tentando resolver? É o registro em si ou a resolução? Essa é a minha primeira pergunta.

E, em relação a isso, uma pergunta sobre desempenho. Quero dizer, hoje, o sistema é construído para ter um desempenho muito bom, porque há milhões de resoluções por segundo, e os sistemas que usam blockchain ou registro de anexos interno, livro-razão de IP, eles são... normalmente, eles devem levar todo o espaço de nomes do domínio para provar algo usando chaves de criptografia, então, como isso funciona? Quero dizer, considerando as limitações sobre desempenho e a limitação do registro somente para anexos.

JEREMY RAND: Sim. Boas perguntas. No que diz respeito ao não determinismo como um problema, o exemplo que dou atualmente é que, quando o encurtador de URL bit.ly foi originalmente registrado, as pessoas que o registraram não pensaram que o domínio .LY pudesse vir a ser controlado pelo Estado Islâmico no futuro. Bem, agora há um risco muito real de que o ISIS possa terminar controlando isso e, enfim, o que acontecerá se eles se apropriarem desse domínio?

Além disso, os registradores de nomes de domínio às vezes cometem erros. Isso é muito mais raro agora do que já foi, mas, no começo do DNS, os registradores de domínios foram enganados para transferir nomes de domínio a outras pessoas

sem a devida autorização, por exemplo, com o envio de faxes falsificados, coisas desse tipo.

Então, eu não acho que haja um risco muito forte necessariamente para casos normais, mas há risco suficiente de que as coisas deem errado, e por isso acho que vale a pena procurar coisas que se comportem de maneira mais determinística.

Quanto à capacidade de expansão, você tem toda razão, as blockchains e estruturas de dados apenas para anexos, em geral, têm uma capacidade de expansão muito mais baixa do que coisas como o DNS, então, sim, você tem toda razão. Sinceramente, não está claro ainda exatamente até que ponto algo como o Namecoin pode ser expandido. Houve uma conversa interessante sobre isso ontem na parte de perguntas de um painel do qual participei aqui. Mas, sim, ele pode ser expandido um pouco mais em relação ao estado atual. Acho que ele poderia lidar com a maioria dos usuários dos serviços .ONION do Tor sem muitos problemas, o que seria uma grande vantagem. Ele poderia substituir totalmente o DNS hoje? Com certeza, não. Ele poderia substituir totalmente o DNS em um futuro distante? É difícil dizer. Talvez sim, talvez não.

DAVID CONRAD: Certo. Obrigado. Acho que já passamos alguns minutos da hora, então o próximo orador é o Paul Vixie, da Farsight Security, que vai falar sobre as zonas de políticas de resposta.

Paul, a palavra é sua.

PAUL VIXIE: Obrigado, David. Bem, já que estamos no assunto de adicionar camadas de bruxaria ao DNS ou ao sistema de nomes em geral, já que ele não funciona como gostaríamos, tenho meu próprio candidato.

O que eu gostaria de destacar, no entanto, é que a ICANN manifestou, vários diretores executivos manifestaram, em vários momentos, que "Nós não somos a polícia da Internet", e isso quase sempre em resposta a alguém que gostaria que a remoção fosse mais fácil, porque há algum nome de domínio em algum lugar que está redirecionando a alguns recursos em algum lugar, que estão causando algum tipo de dano a alguém, e, enfim, a suposição na era pré-Internet é que tudo era de propriedade de alguém e, se algo estava sendo usado para prejudicá-lo, você poderia descobrir quem era e fazer com que fosse preso, processado, ou pelo menos que recebesse sua reclamação e tomasse uma providência.

Então, essa coisa onde a Internet está é... não sei... um serviço de lavagem de responsabilidades onde você pede a remoção de coisas que estão lhe prejudicando, mas acontece que essas coisas não são de propriedade de ninguém, e todos dizem "Sinto muito, não sei a quem você deve recorrer para remover isso, mas não sou eu". Isso é muito frustrante para as pessoas que estão sendo prejudicadas por coisas que estão acontecendo na Internet.

Bem, enfim, podemos reclamar sobre o tempo o quanto quisermos, mas também podemos sair e fazer nosso próprio tempo.

Próximo slide.

Todos os que vejo à minha direita já conhecem tudo isso e todos os que vejo à minha esquerda talvez precisem refrescar a memória. Então, pelo bem do George Sadowsky, vou começar logo com isso.

[Risos]

PAUL VIXIE: Há três camadas no fluxo de dados do sistema de nomes de domínio.

Na parte inferior, estão os resolvedores stub. São todos os nossos smartphones, laptops, as máquinas virtuais, todas as máquinas. Basicamente tudo o que faz uma consulta ao DNS é um resolvedor stub. E ele quer comunicar-se com um servidor recursivo, que, francamente, não é um nome muito bom. Precisaríamos de um departamento de marketing melhor para isso.

Mas, deixando de lado o tipo de recurso sobre o qual estamos falando, vamos pensar nisso como uma palavra em branco. Essa coisa é capaz de responder às suas perguntas, inclusive a resposta negativa de que não há resposta, nome errado ou não há dados, qualquer coisa.

Ele faz isso com um cache à esquerda, o que já é um certo armazenamento. Normalmente, não se trata de armazenamento em disco, conforme mostrado no ícone aqui, mas mesmo assim ele se lembra de respostas recentes, então, se várias pessoas perguntarem a mesma coisa, você não precisará ficar pesquisando na Internet várias e várias vezes.

Porém, se alguém perguntar alguma coisa que não esteja em seu cache, então você terá de fazer isso. Você deverá ir ao primeiro nível, que é onde a ICANN realmente reside. O mundo da ICANN são os servidores com autoridade. Os servidores de nomes raiz, os servidores de TLDs, os servidores de TLDs

eficientes, os registros, os registradores, os registrantes, tudo isso é espaço com autoridade.

Assim, os servidores com autoridade, do ponto de vista do protocolo, são o local onde o conteúdo entra no sistema de nomes de domínio, vindo do exterior. Portanto, uma vez que algo esteja no sistema de nomes de domínio, você pode recuperá-lo usando o protocolo do DNS, mas antes da recuperação isso deve ser importado de alguma forma. Normalmente, a partir de um arquivo de texto, ou de um banco de dados, ou de um software. E esse é o trabalho das autoridades, importar conteúdo do DNS vindo do exterior.

Portanto, o que não é comum nesta apresentação em uma reunião da ICANN é que não vamos falar sobre os servidores de autoridade ou sobre a política pela qual você decide qual nome criar ou quem deve operar o que quer que seja. Enfim, isso é o... normalmente, quando eu costumava participar dessas coisas com mais frequência, passávamos muito tempo falando sobre questões dos servidores com autoridade e das políticas em torno a eles, e certamente é aí que está todo o dinheiro, mas hoje, para variar, vamos falar sobre a camada do meio.

E o motivo disso é que as pessoas que estão sendo prejudicadas pelo uso da Internet como vetor do dano realmente querem poder fazer alguma coisa, mas acontece que você não pode

impedir que as pessoas que queiram prejudicá-lo registrem nomes de domínio e publiquem conteúdos... associem conteúdos a esses nomes de domínio que o prejudicarão. Isso seria uma solução de longo alcance. Se você imaginar que está na margem da Internet e que essas pessoas estão na margem oposta, você gostaria de ter uma solução de longo alcance com a qual poderia impedir, não sei, uma infração de marca seria um exemplo, propriedade intelectual seria outro exemplo, materiais on-line de abuso de menores seria outro exemplo. Há muitas coisas que você considera prejudiciais e que gostaria de impedir que entrassem na Internet, lá no outro lado dela, mas você não pode fazer isso porque, novamente, a Internet funciona como um serviço de lavagem de responsabilidades. E, assim, chegamos, não por opção, mas sim por necessidade, a uma solução de curto alcance, uma coisa com a qual, já que não posso impedir que esse conteúdo seja criado e não posso removê-lo de maneira suficientemente confiável, vou organizar minha forma de ver o sistema de nomes de domínio da Internet para que seja compatível com a não existência do que quer que seja que possa estar me prejudicando.

E isso foi feito com muito sucesso. Começamos esse projeto em 2011. Revisamos o protocolo três vezes, de modo que estamos no Protocolo 4 agora. E, atualmente, estamos buscando padronizar o protocolo atual, e depois disso vamos transferir o

controle sobre o protocolo à IETF, mas por enquanto a IETF não tem muito a ver com isso.

Realmente foi uma espécie de iniciativa privada de uma equipe, não diferente dos projetos de código aberto, como o sistema Namecoin. Portanto, alguns de você realmente contribuíram com ideias e recursos para isso, mas não fizeram isso por meio da IETF, mas sim porque nós pensamos que vocês são inteligentes e têm cuidado com o que dizem.

Portanto, o que estamos fazendo aqui é permitir que sejam usadas a observação e a análise externa para elaborar uma política, e essa política rege a resposta, e chegarei ao "Z" daqui a pouco, mas apenas quero dizer que o cache não é afetado por isso.

Vocês poderiam imaginar uma política que diz: "Caramba, há um novo botnet com algoritmo de geração de domínios por aí e está criando todos esses nomes. É como o Conficker ou algo parecido. E queremos ter certeza de que, se alguém procurar algum desses nomes, não obterá resposta, porque a resposta seria... poderia dizer a um dos meus bots ou a algum cliente infectado na minha rede como alcançar um servidor de comando e controle na rede de outra pessoa, e eu não... eu tenho de interceptar isso em algum lugar. Eu decido interceptar isso no DNS."

Então, talvez você simplesmente diga: “Certo, esses nomes computáveis que o botnet vai usar hoje são proibidos”, e essa pode ser a política que você vai aplicar.

Mas, amanhã, isso já não será válido, certo? Amanhã, haverá um conjunto diferente de nomes. Esses botnets com algoritmo de geração de domínios estão usando a data como parte do cálculo de qual nome usar. Então, não se trata de bloquear um nome para sempre. Isso realmente... isso aumentaria drasticamente a probabilidade de colisão, e há colisões apesar de que esses nomes...

Um botnet com algoritmo de geração de domínios como o Conficker gera nomes realmente feios, mas eles entram em conflito com nomes reais não maliciosos que eu acho feios. Então, esses devem ser removidos.

E, bem, nós não colocamos a política no cache. O que realmente colocamos no cache é a verdade.

Assim, o mecanismo da política de resposta somente afeta o que um resolvedor stub verá. Ele não afeta o que está armazenado ou o que é recuperado das autoridades.

Bem, eu disse que ia falar sobre “Z”. “Z” é a zona que reflete o fato de esses servidores recursivos já estarem presentes na Internet. Há 25 milhões deles, a maioria dos quais não devia

estar lá. São uns pequenos modems idiotas, por cabo, que não deveriam estar executando esse serviço, mas estão. E cerca de 2 milhões deles são internacionais. Portanto, há cerca de 2 milhões de servidores recursivos que são relevantes. E há ainda o DNS aberto e o Google com sua coisa 8.8.8.8. Há muitos servidores recursivos relevantes. E eles são... deixem-me ver... como posso dizer isso?

Queremos poder controlar a política desses servidores usando dados externos, e muitos desses servidores estão nas profundezas de redes existentes, muito bem protegidos por firewalls, de modo que não podem chegar ao exterior ou ser alcançados desde o exterior.

Considera-se uma boa medida de segurança proteger seus servidores de nomes recursivos com um firewall, para que eles não sejam usados como amplificadores de DDOS por pessoas de fora da rede.

Mas observamos que muitos deles têm permissão para comunicar-se com o protocolo do DNS fora da rede, então decidimos que, se pudermos furtivamente incluir a política na forma de dados do DNS para que sejam recuperados pela porta 53 de TCP da mesma forma que são recuperados outros dados do DNS, isso provavelmente funcionaria, e esses servidores recursivos poderiam assinar uma fonte de política. Assim, foi

iniciado o experimento de tentar infiltrar uma política de resposta na forma de uma zona do DNS.

Portanto, isso seria... é a zona mais feia do DNS que vocês jamais verão. É cheia de padrões que propositalmente não ocorrem na natureza, então é realmente artificial e é horrível de se ver.

Você poderia ficar orgulhoso por isso ser tão horrível, como se a feiura fosse em si um projeto de arte.

Então, o fluxo de trabalho aqui é que alguém lá em cima, na parte superior direita, faz a observação e a análise. Essa pessoa pensa: "Certo, um novo botnet, novo DGA, novo conjunto de nomes que não deveria ser resolvido hoje", ou talvez seja um novo bloco de endereços IP que você saiba que está sendo usado por um spammer e talvez ele tenha uma estação de rádio pirata e esteja fazendo propaganda de um espaço de BGP que não lhe pertence, e nós realmente queremos ter certeza de que qualquer resposta que possa resultar de um registro A ou de um registro AAAA dentro desse espaço pirateado não seja dada hoje.

Portanto, você joga todos os resultados dessas observações e análises na zona da política de resposta, a qual é assinada no método de transferência da zona normal por servidores recursivos.

Bem, eu gostaria de ressaltar que esse ato é voluntário. O operador do servidor recursivo deve querer que isso aconteça. Não se trata de SOPA. Não é algo feito a você por alguém que esteja acima e que você não pode evitar.

Além disso, se o seu servidor recursivo for assinante de uma dessas coisas e você não gostar disso, poderá trocar para 8.8.8.8, portanto, isso é voluntário, mesmo para um resolvedor stub. Bem, todo esse método, embora possa ser usado para tentar exercer um efeito sobre a censura, não o é. Ele deve ser visto como uma agregação de valor, caso contrário não será usado nem pelo operador do servidor recursivo nem pelo operador do resolvedor stub.

Então, também quero descartar nisso.

Certo, quais são os números? Determinado servidor recursivo pode estar executando BIND ou Unbound, usando o mesmo software que eu conheço ou o PowerDNS, ou... tem mais um. Há quatro implementações independentes que não compartilham o código fonte entre si, e todas elas interoperam corretamente. No mundo da IETF, se você tiver várias implementações interoperáveis, pode começar a acreditar que talvez o documento do protocolo esteja suficientemente completo. Portanto, com quatro, acho que cumprimos isso.

Há milhares de servidores recursivos que assinam uma ou mais zonas de políticas de resposta. E há cerca de doze provedores de segurança que publicam suas observações e análises neste fórum. O Rod Rasmussen representa um deles, ou representava até pouco tempo atrás.

Mas há um site, o dnsrpz.info, que tem uma lista de todas essas implementações, todos esses publicadores, e tem indicadores para a especificação. E isso é o que a comunidade está fazendo para se proteger o mais próximo possível contra problemas que estão sendo introduzidos à distância, onde não podemos evitá-los. E está funcionando. Está funcionando realmente bem.

Nós... minha empresa agora oferece uma política de segurança nesse formato de zona e ela tem sido bem recebida. Acho que o Rod também teve sucesso com isso na última empresa. Então, é bom para a indústria da segurança, porque traz mais clientes para nossos negócios, e também é bom para as pessoas que estão tentando defender-se, porque lhes oferece um novo gargalo em suas redes e um padrão muito aberto, pois elas podem ter uma solução de vários fornecedores, conforme o conjunto de políticas de segurança que elas queiram assinar.

Por último, mas não menos importante, também é uma solução empresarial. Portanto, embora eu tenha mencionado que o Rod e eu estamos no negócio de vender essas políticas, também é

muito comum que, digamos, um banco tenha uma lista de coisas que eles não querem resolver hoje. E, na ausência dessa tecnologia, eles têm criado zonas vazias em qualquer ponto do espaço de nomes às quais eles essencialmente querem aplicar um pouco de corretor branco e impedir que as coisas fiquem visíveis. Se você está fazendo 6 milhões e está perdendo a metade disso todos os dias, é muita rotatividade na configuração de seu servidor de nomes. Enquanto que, com algo como a zona de políticas de resposta, você não altera a configuração de seu servidor de nomes. Você simplesmente altera a política de resposta. É uma operação muito leve.

Portanto, inevitavelmente, as pessoas que instalam isso, a primeira coisa que elas fazem é criar uma zona local da política de resposta que seja mantida por seu próprio departamento de segurança, de modo que, quando tomarem conhecimento de ameaças – novamente, são observações e análises –, elas podem rapidamente ativar a política de resposta em seu servidor de nomes recursivo em uma espécie de matriz na qual ela é colocada e depois sincronizada em todos os lugares, e então a empresa não responde mais a determinadas perguntas ou não responde mais a perguntas que produziriam certas respostas.

Outras políticas poderiam ser: não responder a nada que envolva um determinado nome do servidor de nomes. Então,

você essencialmente pode envenenar conteúdos sem saber qual é a pergunta ou a resposta; mas você sabe que veio desse nome do servidor de nomes ou de um endereço IP do servidor de nomes dentro de uma determinada faixa, então tem que ser algo ruim. Há muitos nós. Como o David Conrad me disse certa vez, temos corda suficiente para que alguém que queira se enforcar possa fazê-lo.

E acho que a última coisa que falta mencionar é que o que nós basicamente fazemos é dizer: "Quero mentir" e fingir que algo que existe não existe. Em outras palavras, é um sinal sintético NXDOMAIN falso. NXDOMAIN é o valor do código de retorno no DNS que indica que a pergunta que você está fazendo se refere a algo que não existe. Mas isso não é nem de longe a única coisa que você pode fazer, porque muitas pessoas não querem fazer isso. Elas preferem criar o que chamamos de jardim amuralhado, no qual... digamos que você procure um nome do Conficker, um botnet do Conficker com um algoritmo de geração de domínios. Talvez o que você realmente queira é colocar um pop-up na tela de seu usuário que diga: "Ei, você está infectado com o Conficker". E, de fato, você pode fazer isso se... em vez de responder com um NXDOMAIN sintético, você responder com um alias sintético para dizer que o nome canônico do que você está procurando é walledgarden.example.com. Portanto, algum servidor da Web

que seja executado pela própria empresa para dizer às pessoas: "Ei, você provavelmente está infectado, deveria ligar para o departamento de TI agora". Bem, há muitas outras coisas a fazer além de mentir sobre a existência de algo.

E realmente acho que o último tópico antes de passar às perguntas é que estamos mentindo. Tudo isso é mentira. Isso é... a autoridade é de propriedade de alguém que você considera malicioso e não quer saber a verdade. E você decide mentir para si mesmo porque essa é a forma de fazer com que sua rede e seus ativos respondam a uma ameaça em particular. Quando você mente, uma das coisas que se rompe são as DNSSEC. E as DNSSEC são incrivelmente importantes para o futuro da economia mundial. Precisamos tê-las, não apenas para a DANE, mas também para todos os aplicativos que reconhecem as DNSSEC e que estão em andamento, em etapas variadas. E isso se rompe. Se você executar isso e os próprios dados forem assinados pela autoridade, nosso código os ignorará. Nosso código não executará a política em nomes que assinam as DNSSEC. E proporciona aos malfeitores uma forma muito fácil de contornar isso, que é simplesmente atacar as DNSSEC.

No entanto, o resolvedor stub também deveria estar perguntando pelas DNSSEC. Assim, as DNSSEC ainda não são suficientemente onipresentes para impedir que isso seja eficaz.

Mas, em algum momento, isso será um problema. E eu realmente espero que, depois que publicarmos a especificação atual e passarmos o controle para a IETF, haverá quase imediatamente um novo protocolo que será exatamente como este, mas que faça algo um pouco mais sensível com as DNSSEC. Enfim, é um ponto fraco que conhecemos e que não está nos afetando agora. Mas realmente espero que nos afete porque, se isso acontecer, significará que as DNSSEC se tornaram onipresentes, que é o que precisamos. E essas eram as observações que eu tinha preparado, estou pronto para as perguntas. David, quantos minutos temos?

DAVID CONRAD: Provavelmente temos cerca de cinco ou sete minutos para perguntas, Paul. Quem quer começar?

Não há perguntas para o Paul? Certo. Bem, eu começo.

[Risos]

Bem, Paul, acho que uma das implicações da RPZ é que ela de certa forma reforça os problemas que vários dos novos gTLDs estão tendo com a aceitação universal. Primeiro, ela é precisa? E, segundo, tem alguma forma de lidar com isso?

PAUL VIXIE: Bem, tenho um filho que trabalhou no setor de nomes de domínio por um tempo. Quando o domínio .ENTERPRISES tornou-se disponível, ele registrou VIXIE.ENTERPRISES, que eu achei bonitinho, porque eu tinha uma empresa de consultoria antes dele nascer.

Aí, ele tentou usá-lo e descobriu que .ENTERPRISES simplesmente não era um dos padrões que, digamos, a United Airlines esperava que você associasse à sua conta. Felizmente, eu conhecia o cara da United e consegui resolver isso. Mas ele teve todo tipo de problemas. Então, entendo totalmente que esses novos TLDs genéricos são difíceis de usar porque muitas pessoas pensam que poderia ser .COM, .NET, .ORG, .INFO ou alguns códigos de países. E, se não é nenhum desses, então tem que ser um erro de sintaxe. Eu entendo isso. Mas isso não deriva da RPZ, e não ouvi falar desse problema associado à RPZ.

DAVID CONRAD: Certo. Você indicou que a RPZ não funciona com as DNSSEC. Eu pensava que a RPZ funcionava com as DNSSEC no sentido de que, se uma zona fosse assinada e a resposta voltasse para ser validada, ela poderia ser validada. E, depois da validação, a resposta que foi devolvida ao resolvedor stub seria modificada como devidamente indicado pela RPZ.

PAUL VIXIE: Isso é quase verdade. Certamente vai funcionar dessa forma se o stub não pedir as DNSSEC. Se você não definir DO igual a 1, então o que você acaba de dizer é o que vai acontecer. Nós recuperaremos os dados. Nós os validaremos, se possível. Nós os colocaremos no cache. E, então, quando estivermos tentando definir uma resposta para a pergunta original, diremos: "Espere, há uma política". E o stub não solicitou as DNSSEC, então simplesmente vamos inventar coisas, porque se o stub não vai poder dizer se estamos mentindo, então vamos mentir. No entanto, se o stub pedir registros do DNS e houver registros do DNS, não aplicaremos a política.

DAVID CONRAD: George?

GEORGE SADOWSKY: Obrigado, Paul, pela atualização. Estou quase pronto para fazer o teste.

Então, acho que é uma pergunta mais para as pessoas que produzem as informações nas quais a política se baseia.

Falo sobre as considerações de vida útil (TTL, time to live). Com que frequência você precisa transmitir isso? Com que frequência é feita a alteração que você quer dar a seus usuários? Como você sabe qual é a vida útil?

PAUL VIXIE: Certo. Bem, acredite se quiser, fico feliz por você ter perguntado isso. Então, a conexão é ao vivo. Se você fizer uma alteração, como é uma zona do DNS normal, haverá uma notificação, haverá uma transferência de zona incremental e haverá atualizações quase instantâneas. Portanto, na medida em que você mudar de ideia e disser: "Ah, eu gostava dessa política há dez minutos, mas não gosto dela agora", você pode simplesmente mudar de ideia e isso será refletido instantaneamente em sua base de assinantes. É muito importante para nós não romper nada novo. Assim, para isso, se... nós não queríamos nenhum dado velho no sistema. Vou lhe dar um exemplo.

Minha empresa vende um serviço de domínios recém-observados. Isso porque observamos que há 2,5 novos pontos de autorização criados na Internet a cada segundo, e provavelmente a metade deles desaparecerá em 24 horas. E 1/6 deles desaparecerá em dez minutos. É uma taxa de rotatividade muito alta. Essas coisas são criadas com a finalidade de incomodar alguém e são removidas quase instantaneamente em muitos casos, ou são colocadas em listas negras por coisas como a SpamHaus. Bem, isso não significa que tudo que é novo seja ruim, mas significa que há uma probabilidade estatística de que algo que é novo seja ruim.

Como eu me lembro dos bons e velhos tempos em que você pedia um nome .COM e, se fosse depois de terça-feira, você o recebia na sexta, não me importo que os nomes de domínio não funcionem tão bem assim. Toda essa coisa que a ICANN e seu ecossistema desenvolveram de obter em até 30 segundos realmente não tem um exemplo de caso que me preocupe.

Portanto, isso significa que devemos enviar uma atualização por segundo aos nossos assinantes da RPZ, dizendo: “Estes são os novos nomes de domínio que observamos. A propósito, estamos excluindo agora os que têm mais de dez minutos, porque somente os novos interessam e, de acordo com sua definição, já não são mais novos depois de dez minutos.” Temos várias definições.

As redes, enviando uma atualização por segundo, podem sincronizar a política de resposta em milhares de clientes sintéticos ou dezenas de clientes reais. E tudo isso está funcionando. Portanto, isso flui muito bem. Não há nada velho

DAVID CONRAD: Warren?

WARREN KUMARI: Bem, acho que é mais um comentário do que uma pergunta. Eu operava meu próprio servidor de nomes para alguns domínios e

realmente acabei me incomodando com a quantidade de spam, então os desativei.

Depois, comecei a assinar feeds de RPZ de várias pessoas diferentes e os ativei novamente porque, com a RPZ, quase não tenho que lidar com spam, certo? Recebo feeds de spam de algumas pessoas com a RPZ. Mas ela cuida do assunto e agora tudo funciona novamente. Isso é...

PAUL VIXIE: Obrigado por dizer isso. E permita-me que comente seu comentário.

Você não consegue fazer as coisas funcionarem na Internet, a menos que o DNS funcione. Sei que há vários protocolos ponto a ponto por aí, portanto, nem todas as pessoas do BitTorrent perceberiam quando o DNS não funciona. Mas, para o resto de nós, se o DNS não funciona, não importa o que possa ser acessado, porque não vamos digitar endereços IP. Certamente não vamos digitar endereços IPv6.

Bem, essa propriedade também funciona para os malfeitores. Não são apenas os bons que não conseguem fazer as coisas se o DNS não funciona. Os malfeitores não podem ser acessados se não estiverem no DNS.

E você mencionou o spam. Para mim, isso significa que spam por e-mail [inaudível].

Tenho meu servidor de e-mail, o Postfix, e ele está conectado de modo a tentar pesquisar no DNS cada nome no cabeçalho, cada nome no envelope e cada nome no corpo. E, se algum deles falha, eu rejeito o e-mail, o que significa que usar esse gargalo simplesmente como uma forma de dizer que esses nomes não deveriam existir e, se eles realmente existirem, então mentir e dizer que não, causará a ocorrência de todo tipo de falhas em sua infraestrutura. É preciso estar preparado para isso. Pode ser um pouco surpreendente não receber tanto spam. Na verdade, o que você disse é uma tentativa secundária de toda essa iniciativa.

DAVID CONRAD: Certo. Obrigado, Paul, por sua apresentação sobre a RPZ, e agora passamos a palavra ao Paul Wouters.

PAUL WOUTERS: Obrigado.

Já que estou com o microfone, um pequeno comentário. Devo dizer que o Paul Vixie e o John Gilmore são as duas pessoas mais difíceis de se mandar um e-mail no planeta, por causa de todos os mecanismos de defesa ou falta de defesa que eles utilizam.

Então, com isso...

>> (Fora do microfone.)

PAUL WOUTERS: Sou um dano colateral feliz.

Bem, conseguir a implementação das DNSSEC em grande escala tem sido um problema. O registro de DS que as pessoas precisam para entrar na zona pai é um processo muito difícil que envolve muitos seres humanos, e o ser humano mais importante está trabalhando no registrante e realmente não sabe nada. Ele simplesmente comprou um serviço e um nome de domínio e não sabe nada. Ele apenas quer que isso funcione e ele tem um operador de domínio que executa tudo para ele. Então, eles nem sequer sabem o que são as DNSSEC e não sabem como ativá-las, e mesmo que seu operador do DNS lhes disser o que fazer, eles vão ter muita dificuldade para fazê-lo.

Portanto, há muitos domínios que em vários... provedores de alojamento muito grandes que são basicamente assinados, mas não autorizados com um registro de DS, então, mesmo que sejam protegidos por si mesmos, são uma pequena ilha, porque há... esse registro de DS não entrou no diretório pai, porque não há maneira de fazer isso.

E, assim, esse problema precisava de uma solução.

A IETF primeiro se esquivou de resolvê-lo, mas, em um momento determinado, o problema tornou-se tão grande, que eles voltaram atrás e... isso é confuso. Vou fechar meu laptop.

Bem, as duas coisas que eles precisavam fazer – e isso é feito agora na RFC-8078, que foi publicada na semana passada – é que eles devem ter alguma forma para que o operador do DNS indique ao registro que esse domínio tem agora um registro de DS e se ele pode publicar esse registro de DS.

E a outra coisa que os operadores de DS também precisam ter é uma forma de dizer: "Meu cliente está indo embora; meu cliente não quer mais as DNSSEC". Também precisamos ter uma forma de dizer ao registro que remova novamente esse registro quando as DNSSEC não forem mais necessárias.

Enfim, esta RFC basicamente possibilita que isso seja feito. O que ela faz é criar... ela usa o tipo de registro CDS, que é basicamente o mesmo tipo de registro do DS, mas é publicado no lado do cliente, portanto, na própria zona do cliente.

Assim, uma vez publicado ali, você encontra uma forma de entrar em contato com seu registro e dizer: "Ei, publiquei este registro de CDS. Você pode dar uma olhada nele e, se estiver de acordo, publicá-lo como um registro de DS em sua zona pai?"

Enfim, isso é o que esse novo registro faz.

Desculpem. O registro não faz isso. O uso disso aqui é novo.

Há várias formas pelas quais você poderia entrar em contato com seu registro, e elas ficam para outras versões. Atualmente, há outra versão em andamento, por exemplo, que usa uma interface tranquila, que usa HTTP, para transmitir essas informações, mas poderiam ser inventados outros mecanismos para isso também. E o registro de desativação especial é o registro de CDS com todos os zeros, que basicamente significa: "Por favor, desative isto, não queremos nada".

Há um erro de digitação no slide. Deveria haver um quarto zero, que também é um problema na última revisão da versão. Percebemos isso a tempo para a publicação da RFC, mas, obviamente, não atualizei meu slide.

Enfim, o sistema funciona. Como agora há novas extensões de EPP, o registro, uma vez que tenha aceito esse tipo de atualização fora dos limites do operador do DNS, pode avisar isso ao registrador, de modo que ele também esteja ciente de que este registro foi atualizado e não entrou por meio de uma transmissão tradicional de EPP.

E isso está sendo atualmente implementado ou em fase de implementação para vários TLDs, então, isso significa que, em

breve, haverá centenas de milhares mais de domínios autorizados que assinam as DNSSEC, e isso será um grande salto na implementação das DNSSEC e, sim, esperamos que isso seja um grande sucesso.

DAVID CONRAD: Certo. Alguma pergunta para o Paul?

Sim, Liman.

LARS JOHAN-LIMAN: Apenas um... aqui é o Lars Liman. Apenas um rápido esclarecimento. Trata-se dos registros de CDS propostos por... foi o Olaf Kolkman? Ou aquele que está circulando na IETF?

PAUL WOUTERS: Sim. Trata-se da RFC do Olaf Kolkman, quero dizer, sim.

LARS JOHAN-LIMAN: Muito bem. Obrigado. E também, isso direciona um pouco o foco para a falta de relacionamento formal entre os operadores do DNS e os registros, eu acho, o que é bom.

PAUL WOUTERS: Eu não mencionei essa palavra de propósito.

DAVID CONRAD: Patrik?

PATRIK FALTSTROM: Vocês têm analisado...

À sua esquerda, aqui.

[Risos]

PATRIK FALTSTROM: Bem, o que aconteceu no caso normal... você pode voltar ao slide, por favor?

No caso normal, a transação das DNSSEC é feita por meio do registrador, então ele tem toda a responsabilidade final de garantir que tudo que diz respeito ao registrante esteja concluído, inclusive a chave... o material de chave.

Neste caso, a atualização da chave passa do operador do DNS para o registro sem passar pelo registrador, certo?

PAUL WOUTERS: Correto.

PATRIK FALTSTROM: E o que você está dizendo é que isso é acionado por meio de um evento no EPP, certo?

Então, o registrador deve usar o comando puxar nesse caso para recuperar as informações sobre o novo material de chave.

É essa a intenção?

O que me preocupa é que o registrador de repente não tenha uma visão completa da zona, em cujo caso... isso poderia afetar as responsabilidades do registrador em relação com o registro.

PAUL WOUTERS: Correto. Sim. Mas, pelo que eu entendi, havia uma nova extensão do EPP que permitia que o registro empurrasse, então não é que o registrador precise puxar.

PATRIK FALTSTROM: Com certeza. Há extensões com as quais é possível fazer isso. Mas há... no projeto normal do EPP, todo o projeto é para que os registradores atualizem o registro, e não o contrário.

PAUL WOUTERS: Correto.

PATRIK FALTSTROM: Certo. Bem, essa é ainda outra coisa na qual o registro está prescrevendo uma alteração na máquina de estados no registrador, e temos muito poucas delas, e essa é outra, certo?

PAUL WOUTERS: Certo. No entanto, o registrador também poderia ter compatibilidade com o mesmo mecanismo e conseguir que o registrante fale com ele.

Então, para aqueles que estão pensando em implementar todos os requisitos das DNSSEC que não precisam desse contorno, não seria necessário fazer a máquina de estados. Isso é... desde que o registrador e o operador do DNS tenham um bom relacionamento de trabalho, que possam conversar entre eles. Porque se o registrador não puder conversar com o operador do DNS, o problema continua sendo que eles não conseguem transmitir essas informações, a menos que usem este mecanismo.

PATRIK FALTSTROM: Posso falar com você como se estivesse usando uma consulta ao DNS, certo?

Enfim, para fins de transparência, quando revisei este documento, sugeri que ele fosse... que ele padronizasse este

excelente registro de CDS, independentemente de ser o registro ou o registrador quem vai puxá-lo.

PAUL WOUTERS: Onde o registrador publicaria isso? Você quer dizer, se o registrador enviar isso pelo EPP?

PATRIK FALTSTROM: Não. Publicar... o registrador recupera o novo DS do operador do DNS e o empurra para o registro usando o EPP.

PAUL WOUTERS: Eles já podem fazer isso sem esta versão.

DAVID CONRAD: Então...

PATRIK FALTSTROM: Vamos falar sobre isso off-line. Sim. Eu já expliquei isso uma vez na lista de e-mails da IETF e provavelmente não precise fazer isso aqui de novo.

DAVID CONRAD: Certo. Dan e depois Warren.

DAN YORK: Bem, eu queria apenas agradecer ao Paul por apresentar isso, e acho que o ponto principal, talvez, para os membros da diretoria da ICANN e para o resto das pessoas que estão ouvindo e que não querem entrar nos detalhes disso é apenas perceber que faz parte de um trabalho em andamento para proporcionar uma automação melhor para a forma de funcionar das DNSSEC, porque, certamente, se observarmos as implementações em grande escala das DNSSEC por parte de operadores do DNS ou de outras pessoas que tentam fazer isso, uma das grandes barreiras que foram identificadas foi a transmissão dessas informações, desses registros de DS, até os registros.

Então, esse é um dos mecanismos que estão agora disponíveis para os registros que decidirem usá-los a fim de ajudar na automação dessa publicação de informações e melhorar isso, o que levará, afinal, a um DNS mais seguro.

Portanto, esse é realmente o ponto principal de tudo, é um mecanismo novo que está disponível agora e, assim, os registros podem considerá-lo como uma forma de fazê-lo funcionar.

Quanto ao que o Patrik colocou, os registradores também podem considerar isso.

DAVID CONRAD: Warren?

WARREN KUMARI: Bem, o motivo pelo qual eu tentei interromper o Patrik é que acho que as pessoas estavam falando com objetivos contrários.

Também acho, Lars, você disse que a versão original era do Olaf. Na verdade, é Olafur, eu acho, o autor original... sim. O Olafur e eu fizemos isso. Sim.

Então, o documento original não conseguiu impedir que as pessoas publiquem esses registros automaticamente. Você precisava ir pelo registro ou registrador, que acho que era sobre o que o Patrik estava falando. Deixamos de fora especificamente a parte "você pode ignorar seu registrador" por causa das mesmas preocupações que o Patrik manifestou. Esta versão melhora a anterior e adiciona novos recursos. Ou talvez eu tenha entendido mal sua...

PATRIK FALTSTROM: O que estou tentando fazer é simplesmente separar o recurso técnico, que é a capacidade do operador do DNS de avisar que isso é um novo material de chave do possível impacto da política referente ao relacionamento entre o registrante, o registrador e o registro. Essa é uma discussão completamente diferente, que poderia ser complicada em determinados TLDs.

DAVID CONRAD: Apenas uma resposta rápida? Sim.

>> Patrik, a questão fundamental que precisa ser resolvida é descobrir quem é o registrante, qual é o identificador especial para conversar com ele. Temos um número limitado de registros, então eles são convenientes como ponto de partida para conversar, mas se pudermos, de alguma forma, entrar no RDAP ou em outro protocolo, encontrar o identificador especial da entidade que deseja conversar conosco, preferentemente o registro ou um revendedor mesmo, ou o revendedor de um revendedor, é isso que ninguém consegue encontrar hoje.

DAVID CONRAD: Dmitry?

DMITRY KOHMANYUK: Olá. Apenas queria fazer um comentário rápido sobre a caixa de registro duplicada e por quê. Suponho que seja um erro de digitação. Segundo, eu provavelmente concordaria com o comentário do Patrik Faltstrom de que, sim, o modelo do EPP... e, a propósito, eu represento um dos TLDs, ccTLDs. Executamos o EPP. É a Ucrânia. Acho que o modelo, quando o estado é dividido, é muito ruim. Também acho que o modelo para puxar é muito ruim e não é dimensionável. No entanto... e, sim, o EPP

é compatível com atualizações de DS, mas meu maior problema aqui é que estamos tentando separar o DNS... desculpem, o gerenciamento do registro de NS e do registro de DS. Isso é ruim. Porque a alteração do operador do DNS pode envolver tanto uma alteração do registro de DS como uma alteração do registro do DNS. Por algum motivo, parece estranho que as atualizações devam [inaudível] esta versão sem supervisão do registro do DNS.

Então, eu diria que você deve voltar ao esquema e ver como essa separação de registrador, digamos, atualização de dados sobre nomes de entidades, endereços e coisas do tipo em relação aos dados técnicos. Sim, é uma boa ideia perder um operador técnico terceirizado, mas a questão é a solução errada, além do que a falta de relacionamento contratual entre o operador do DNS, um ou dois, e o registro é a solução errada, e não é a forma de resolver isso, não é a forma de tornar a Internet mais segura.

Então, sim, boa tentativa, mas eu iria apenas...

PAUL WOUTERS: Bem, vou apenas... uma observação bem rápida e passo a palavra para o Paul Vixie.

Tem havido uma longa discussão na IETF sobre acionadores e temporizadores, então não vamos repetir isso de novo.

É uma opção que os registros podem decidir escolher e, se alguns registros contratualmente não puderem fazer isso ou não quiserem fazer isso, tudo bem, mas será uma opção útil para uma grande quantidade de pessoas que atualmente não podem empurrar registros de DS para seu devido lugar.

DMITRY KOHMANYUK: Bem, sim. Há muitas questões. Acho que não devemos discutir isso aqui. É melhor fazer isso no ambiente da IETF. Obrigado.

PAUL WOUTERS: Certo.

DAVID CONRAD: Paul?

PAUL VIXIE: Eu ia ampliar essa questão. O NomCom trabalha duro para conseguir as pessoas mais qualificadas que estejam dispostas a fazer parte desta diretoria e elas não são necessariamente tão técnicas como as pessoas que estavam usando a Internet nos anos antes da ICANN existir. Devemos usar o tempo delas com sabedoria e respeitar seu tempo, então, se vocês pudessem

ajustar seus argumentos a um nível que o George Sadowsky possa entender.

[Risos]

DAVID CONRAD: E, com isso, passamos agora a outro assunto.

Enfim, foi uma tentativa de reestruturar de alguma forma a maneira de operar do TEG. Fornecemos documentos informativos de uma a duas páginas aos membros da diretoria antes da reunião e eu estava aqui me perguntando se isso é bom ou se devemos continuar tentando evoluir o TEG de maneira a torná-lo mais útil para os membros da diretoria.

E vocês podem responder a isso agora ou enviar-me um e-mail, ou ainda caçar-me no coquetel que vamos realizar em seguida. Os ônibus saem daqui a 15 minutos. E, com isso, declaro encerrada esta sessão do TEG e agradeço a todos por sua participação.

[Aplausos]

[FIM DA TRANSCRIÇÃO]