HYDERABAD – Encontro Conjunto: Diretoria da ICANN e TEG (Grupo de Especialistas Técnicos)
Terça-feira, 8 de novembro de 2016 – 16h30 às 18h30 IST
ICANN57 | Hyderabad, Índia

DAVID CONRAD: Nós vamos iniciar daqui a poucos minutos e se há algum membro do TEG nós ainda temos espaço aqui.

O senhor Göran Marby entrou na sala.

Bem-vindo a todos. Reunião o grupo de especialistas técnicos. Reunião conjunta com a diretoria da ICANN. Temos uma pequena mudança na agenda que o tópico de arquitetura foi retirado porque a pessoa que iria apresentar está se sentindo mal e não vai apresentar.

Então essa é a agenda e o Warren vai falar sobre as questões de IEFT. Para aqueles que não sabem o que é o TEG, está enfocado em questões de tecnologia, especialmente como afetam o uso de identificadores únicos da internet e nós achamos que isso deve ser levado em consideração pela diretoria quando tomar decisões, não é um conselho consultivo, não tem orçamento. O que faz com que não haja obrigação da diretoria de implementar as recomendações.

A agenda dessa reunião, nós temos uma atualização sobre nomes especiais, qual é a situação do problema e o espaço de problemas do SSAC apresentado pelo Jim Galvin e depois o Howard Benn vai falar sobre a virtualização da função de rede. John Levine vai falar sobre o DNSEXTLANG. Warren vai falar de questões relacionadas ao IEFT.

Então vou passar o microfone para o Jim.

JIM GALVIN: Muito obrigado David. Eu estou vendo que o slide está aqui.

Estou fazendo essa apresentação hoje como vice-presidente do SSAC, eu também sou presidente do grupo de trabalho que está trabalhando com essa questão. O SSAC está pensando na questão do espaço e nomes de domínio e a colisão pelo uso da comunidade. Então essa atualização é importante porque chegamos a um consenso quanto às palavras usadas para definir esse espaço de nomes.

O que é o espaço de nomes de domínios? São todos os possíveis nomes de domínios, a partir de uma hierarquia em forma de árvore de rótulos individuais. O DNS, quando se pensa, é na verdade um subconjunto do que estávamos falando. O espaço de problemas é todo o conjunto de domínios e o DNS é só uma parte disso.

O que é interessante observar na comunidade é que o espaço de nomes de domínio e que o protocolo do DNS que suporta isso lida com outras coisas além do DNS público e global.

A razão das colisões é que os nomes de domínios DNS tem tido tanto sucesso que foi adaptado e adotado para usar em outros lugares por outras pessoas, isso é muito bom, é um marco de sucesso, é uma oportunidade de inovação e a última coisa para entender sobre o espaço de problemas, os nomes de domínios são determinados pelo IEFT e não podem ser rigidamente definidos na prática. Então se há um nome e esse existe não tenho informações suficientes para saber tudo sobre ele.

Então quando você tem um browser, você digita algo, então você tem aí a oportunidade de digitar alguns nomes ou colocar um ponto que pareça um nome de domínio e você busca no DNS.

Em geral, isso não é suficiente e os browsers tem que adivinhar como fazer isso. Por exemplo, no seu ambiente local, você tem um resolvedor do DNS e que há outras aplicações. Você tem o mesmo tipo de problema, talvez você não tenha informação suficiente se o nome apresentado, o que parece um nome de domínio, está onde pertence e esse é o espaço de problema com que estamos trabalhando e que a comunidade deve levar em consideração.

Nós fazemos as seguintes observações em relação a isso. Quais são as circunstâncias e os fatos que estão ocorrendo? Então é falta de informação no uso do espaço de nomes de domínio que causa problemas. Com isso há colisões, então há nomes de domínio e uma aplicação que entende isso está usando nomes de domínio e também ambientes locais que usam domínios que devem se referir a coisas no DNS global.

Então há uma colisão, uma aplicação recente ou foi aberta uma rodada de inscrições para novos gTLDs e alguns nomes foram reservados e ainda vão determinar o que fazer com elas. São nomes corporativos e aplicações de e-mail e há certa ambiguidade do que fazer com isso, a falta de coordenação de vários grupos no espaço de nomes cria instabilidade, ambiguidade e isso é um problema e a ambiguidade causa instabilidade e problemas de segurança.

Então o SSAC faz recomendações para a comunidade, analisa esses problemas e identificamos essas coisas para a comunidade para que esta desenvolva processos e políticas para esse tipo de coisa.

Há claramente 2 grupos pelo menos que podem influenciar nos nomes. Uma é a ICANN, porque seu papel como coordenador da designação de nomes que entraram na zona raiz. A ICANN toma essas decisões e o IEFT é outro exemplo de uma organização

que tem um papel e cria uma lista do que chama de uma lista de nomes reservados, são as listas que devem ser avaliadas em tempo para avaliar na verdade os seus problemas sérios. Por exemplo, o .ONION é um exemplo, então nós temos que definir políticas para determinar o que deve existir na zona raiz ou não.

Há indivíduos em instituições que talvez não conheçamos que são usuários privados e esse é o problema que o .crop . mail porque há muitos usos privados desses rótulos que eles colidem com nomes que podem estar na zona raiz e a ICANN como comunidade tem que decidir junto com a diretoria e os funcionários, nós temos que decidir o que fazer com isso e lidar com essa instabilidade.

Eu acho que esse é o último slide, essa é a situação do que nós achamos, o que é o espaço problema, mostrando os achados e a próxima etapa é determinar recomendações e vocês estiveram no fórum público do SSAC, na última sessão nós dissemos que o SSAC espera ter um conjunto de recomendações e um produto de trabalho até o final desse trimestre.

Em relação a isso há alguma pergunta? Em relação a isso.

DAVID CONRAD: Eu gostaria de abrir o microfone para perguntas a esse tema.

STEVE CROCKER: Muito obrigado Jim, ajudou muito.

PETER KOCH: Jim, você apresentou essa visão do mundo, de que há domínios ou espaço de nomes de domínios e há separadas responsabilidades dentro do sistema de domínios, dentro da ICANN e outra responsabilidade do IETF é de quem é essa visão do mundo.

JIM GALVIN: O que nós sabemos é que a ICANN tem a responsabilidade pelos nomes que entram na zona raiz e observamos que há outros grupos que estão tirando vantagem disso, da existência dessa tecnologia, especialmente o DNS público e o protocolo de resolução e utilizam esses nomes em outras partes e nós simplesmente estamos reconhecendo que eles existem e acho que nós temos que reconhecer que existem e a ICANN como empresa e como comunidade precisa reconhecer a sua existência e reagir de alguma forma.

Quem somos nós? A comunidade. Nós. Eu sou parte da comunidade.

PETER KOCH: Jim Galvin, poderia dizer o que é esse pessoal?

Essa questão não é uma questão controversa. O que você chama de uso privado eu poderia dizer que seria uma ocupação, quer dizer, da mesma forma que eu posso usar o seu carro sem o seu consentimento e declarar isso que é o uso privado do carro.

Há um MoU entre a IETF, a ICANN e uma clara separação de responsabilidade para o espaço de nomes e o documento no qual o IEFT e as partes do IEFT tem a capacidade e poder de designar nomes declarando uma questão de protocolo.

Então eu peço que a ICANN e o IEFT tomem uma posição.

JIM GALVIN: Muito obrigado Peter.

Eu vou levar esse comentário para o SSAC para considerações.

STEVE CROCKER: Vamos continuar.

Na verdade é ao contrário Peter.

Eu não estou ciente 100% desses problemas, mas eu gostaria de acrescentar algumas coisas.

O que entra na zona raiz e o que se pode falar do sistema de nomes de domínios entra e sobre o que entra na zona raiz e o

IEFT estruturou o espaço de nomes e você falou no uso de nomes fora do DNS e o problema prático é que nomes que devem ser usados no DNS aparecem de qualquer forma no DNS. Por exemplo, o host local. Então o problema prático é que, embora teoricamente o uso do espaço de nomes usado para outros propósitos e para o sistema de nomes de domínio são completamente... eles se misturam, então nós não devemos ignorar, então temos que prestar atenção em quais são os fatos e se há nomes que aparecem frequentemente tendo acesso a raiz.

Então temos que saber exatamente como é que isso funciona e decidir o que vamos fazer com esses nomes, se vamos proibir ou ter alguma medida de mitigação.

O que eu sei é que o IEFT não está concentrado, não tem nenhuma política específica. Eu não quero dizer aqui o que o IEFT tem que fazer, mas em geral eles não lidam com elaboração de políticas. Então eles não levam em consideração o que você chamou de ocupar.

Então isso pode ser usado como exemplo .ONION. Como é que essas peças se encaixam na sua cabeça?

PETER KOCH: Muito obrigado por ter corrigido a analogia.

Podemos começar daí. Vamos supor que alguém ocupa a terra e que essa terra já não está disponível para ninguém mais e aqui entra a coordenação e a responsabilidade deve ser bem clara aqui.

Aqui não se trata de ignorar os fatos, o tráfego, também isso acontece com os endereços de IP forjados e não é o que sugerimos aqui não. As pessoas declaram seus endereços e depois eles voltam e esses endereços que eles usurparam ficam como algo legítimo e aqui entra um conflito e o conflito aqui é que não existe uma coordenação entre os 2 órgãos. Temos espaços enormes que parecem com um lugar de nomes de domínios, parece mais não é. Então as responsabilidades aqui tem que ficar bem definidas, isso não está acontecendo aqui.

WARREN KUMARI: Queria saber se o IETF tem falado sobre isso recentemente, eu quero que vocês saibam disso. Ele adotou uma declaração recentemente e há consenso que ainda não chegaram a uma decisão definitiva, mas bom, agora parece sim que houve algum consenso, que o processo foi estendido sobre adotar os nomes especiais. Estamos preparando um documento de SSAC que está se conversando sobre esse tipo de coisa com coordenação e o documento de IEFT vai mencionar também essas questões. Estamos avançando agora e essa é a situação.

DAVID CONRAD: Muito bem.

JONNE SOININEN: Seria bom então dividir aqui essas questões, aqui Jim disse que há diferentes categorias, uma é raiz, os números especiais e depois os squatting, de usurpação. O uso privado pode estar em outra classificação que não essa, então o uso privado ninguém controla, mas isso esteve e quanto ao uso especial de nomes talvez nem todos saibam, mas essa é uma coisa que eles não estão na raiz, não podem ser resolvidos no DNS. .LOCAL, por exemplo, pode ser resolvido através de uma coisa que pode ser o DNS multicast e a raiz .ONION que foi uma das últimas que foram alocadas e há poucas que foram alocadas nos últimos anos. Não sei se há outro exemplo como esse.

Essencialmente é .LOCAL .ONION mas isso foi antes de que se tivesse feito alguma política e nenhuma dessas aqui que são reservadas podem ser resolvidas pelo DNS e como dizem o seus nomes são de uso pessoal e a IEFT teve um processo, uma política pelo qual alocava os nomes de uso especial e como .LOCAL, .ONION que ficaram reservados e não pareciam adequado.

Quanto a coordenação no começo, quando começou a trabalhar o IETF sobre política, sobre nomes especiais eu era uma pessoa de contato com a diretoria da ICANN e a GNSO e é verdade que a continuação talvez não seja perfeita, mas sim há pessoas da comunidade da ICANN, também da organização da ICANN que estão trabalhando nesse sentido e acho que pelo menos há algum grau de coordenação, mas de acordo com o que squatting estão fazendo é bastante provável que nesse proposta haja um grau maior de coordenação e eu concordo com você que aqui há algum grau de problema, mas talvez você aqui esteja implicando que haja alguma outra coisa mais a adicionar, tentemos não monopolizar o microfone.

PETER KOCH: Eu vou tentar não monopolizar, vou tentar falar breve,. Isso significa que não pode já entrar na raiz, como reservados, mas não há um documento específico que determine a limitação de fazer coisas na raiz. Temos, por exemplo, um elemento de protocolo que poderia afetar um nome de domínio em segundo nível num TLD já existente.

Essa seria uma maneira de declarar o protocolo para uma sequência de um nome de domínio que não poderia ser resolvido já em um espaço de nomes de domínio, isso seria uma

maneira de bloquear uma parte do espaço de nomes e determinar que tudo que está embaixo disso é importante.

Uma questão que tem a ver com normativas não é uma questão apenas técnica, mas é também uma questão normativa.

JONNE SOININEN: Sim, muito bem, acho que concordamos com isso. Acho que porque o IEFT está trabalhando é justamente para resolver isso. Se é verdade deve existir um diálogo entre a ICANN e o IEFT eu concordo com você.

DAVID CONRAD: Warren.

WARREN KUMARI: Sim, eu justamente pensava em opinar igual.

PETER KOCH: Nós adotamos um documento e determinamos que deveria haver uma relação para coordenação e o IEFT já está trabalhando nisso, temos adotado um documento, estamos avançados e o que vocês estão mencionando aqui me confunde. Desculpem.

É apenas uma coisa que eu mencionei. A comunidade da ICANN está trabalhando nisso, o SSAC está trabalhando claramente nisso e há trabalhos que estão sendo feitos, então ainda podemos melhorar aqui essa questão.

RON da SILVA: Obrigado.

Esse diálogo é muito bom, mas eu entendo que se vocês tiverem tentando estudar e além do espaço reservado específico entre o IEFT e a ICANN deveríamos observar mais amplamente o espaço de nomes.

Há empresas com fornecedores de equipamentos de consumidores que poderiam injetar coisas no espaço de nomes de domínios e colocar coisas parecidas ou que já está no DNS. Isso me lembra sobre algumas dessas vias que me tinha no espaço para registros que tinham endereços que nunca foram roteados e que talvez haja pessoas que possam utilizá-los, estejam utilizando esses endereços e não sabemos, mas é mesmo problema, temos uma colisão e tudo isso é um mercado de transferência que está acontecendo no mundo que vem de compra de uma companhia de outro provedor de serviços para outro e que então aqui precisamos de coordenação, mas também o fato de termos nomes no espaço exige que haja cooperação, coordenação também entre os operadores de

registros de registers e também termos de condições de contrato e com essa combinação se não houve essa recomendação e voltando para a analogia dos números não haverá garantia nenhuma e haverá colisões e usurpação também.

DAVID CONRAD: Kaveh.

KAVEH RANJBAR: Eu tenho um exemplo melhor para comprar isso com o IEFT.

Há alguns anos a APNIC estava assinando um contrato com o 1.2.3.4 que fez uma matéria sobre isso com 500 mega de tráfego e decidiram reservar o espaço e isso se aproxima da nossa opinião consideramos que é a raiz.

JIM GALVIN: Obrigado.

Quanto ao que SSAC pensou a dizer a maneira em que estamos observando isso, aqui há espaço para problemas e muito problemas, é a maneira que estamos abordando as recomendações é considerar o que está dentro da incumbência da ICANN. É fácil de sugerir que, bom, vamos recomendar, parece uma recomendação bem natural, mas vamos nos

confrontar com perguntas lógicas, quem vai coordenar? Por exemplo, e porque e há muitas pessoas que usam nomes de domínios para seus próprios fins e claramente aqui não se trata de coordenar o tempo inteiro e com todos e dessa maneira não vamos resolver o problema em geral, mas a ICANN deve considerar aquilo que pode realmente controlar e aquilo que já está sendo controlado e há problemas sobre o que acontece se alguém chega e tem já uma lista de nomes novos que cria colisões e ambiguidade e o que a comunidade da ICANN e a SSAC e a ICANN como um todo deve proteger é a estabilidade, usando na tecnologia racional.

Devemos considerar então e a comunidade da ICANN deve considerar como quer responder a presença dessas outras listas e usos que aparecem que vão aparecendo às vezes e surgem novas organizações que tem seus próprios processos.

A ICANN deve ter um processo pelo qual reconheça que essas situações podem acontecer e queremos recomendar a comunidade da ICANN e a diretoria mais diretamente esse tipo de situação.

Muito obrigado.

DAVID CONRAD: Como o SSAC está encarregado dessa questão seria bom que esperemos qual é a opinião do SSAC sobre essas questões e o grupo de especialistas técnicos também e outra coisa que eu destaco é que eu acho que o RFC 2860, que é uma maneira de entendimento entre o IEFT e a ICANN determinar que o IEFT tem a capacidade de declarar um protocolo, mas isso vai além da questão de políticas.

A ICANN deve lidar com mais aspectos aqui. Isso traz muita complexidade e eu vou passar para o seguinte item da agenda que eu não me lembro bem qual é.

Eu acho que é o Howard. Howard, por favor, você quer falar sobre a virtualização, a função de virtualização?

HOWARD BENN: Por favor, podem colocar os slides.

Próximo. Obrigado.

Então, vejamos, como alguns de vocês sabem a organização de padrões que determina padrões para a comunidade de celulares e estabelece protocolos ou padrões para a telefonia fixa e móvel.

Bem, nos últimos 10 anos passamos de um mundo de telefones celulares que faziam apenas ligações e agora utiliza para

acessar outras mídias e também a internet. Temos 8 bilhões de usuários com chips, há uma enorme conectividade da internet e dentro das redes nucleares há muita discussão, será que podemos alavancar o trabalho da indústria da internet?

Usar centro de dados para controlar as nossas comunicações e não usar o hardware proprietário de hoje e o IEFT tem trabalhado com isso nos últimos anos e geraram especificações de 2 fases, então na 3ª fase no momento, há vários problemas que apareceram e eu achei que seria útil para informar a comunidade e eu vou falar sobre problemas no final.

Então nós compartilhamos ou computamos o armazenamento nos centros de dados hoje. Há algumas palavras utilizadas e alguns conhecem e eu achei importante mencionar, nós temos o gerente da entidade que vê como que a rede funciona. É um software que roda e que realiza funções em software e em hardware nós compartilhamos os recursos e isso é gerenciado através de orquestração e há um gerente que gerencia os ciclos de vida, o VNF e o que nós temos feito é mapear o excelente trabalho que a comunidade da internet fez nos últimos anos e as políticas dentro e mapear isso dentro do mundo da telefonia móvel.

Em primeiro lugar é a confiabilidade. É muito interessante a percepção da confiabilidade. Nesse momento ainda estamos no

processo de saber com o que as pessoas ficam satisfeitas e se o seu telefone não funciona por falta de cobertura elas reclamam ou se o telefone tem cobertura e não consegue completar a ligação isso é um grande problema e se nós olharmos o número de telefonemas se vê hoje que já diminuiu e quanto à conectividade com a internet os usuários querem confiabilidade, eu não sei exatamente de onde que vieram esses números, mas a maior parte das redes móveis são minutos de tempo sem conexão em um ano.

Os números mostram que a comunidade da internet não é assim exatamente confiável. Nós queremos garantir que haja interoperabilidade entre os diferentes sistemas e é aí que entram os padrões mundiais para garantir protocolos que diferentes revendedores forneçam diferentes partes da infraestrutura e que trabalhem juntos de forma interoperável e confiável.

O que nós fizemos também é como fazer o benchmark desses sistemas, como trabalhar com coisas como confiabilidade e há problemas de latência. Temos um serviço a base de voz que é incriptável, a latência é muito importante, a latência tem que ser muito baixo e isso é importantíssimo e esses serviços tem que ser comparados e em relação a segurança há uma grande preocupação.

Se você tem um operador de telefone que tem seu próprio centro de dados, que não tem acesso ao mundo externo então você tem um centro de dados que possivelmente tem um sistema publicamente abordável que pode estar aberto a cyber ataques. Então há uma grande preocupação dos operações com isso e há grupos de segurança que estão tentando propor soluções, mas nós precisamos trabalhar junto com a comunidade da internet sobre isso.

Outra área muito interessante é no mundo de comunicações por voz nós temos interexecução legal que é uma exigência na maioria dos países que nó operamos. Isso está começando a tentar também na comunidade da internet, talvez possamos compartilhar parte das nossas experiências, vendo o TC Cyber que vê todas as questões de cyber segurança, então como fazer isso e ao mesmo tempo manter a privacidade e a segurança.

A migração é outra área muito interessante e os sistemas não querem ficar fora do ar e começamos a trabalhar mais com as comunidades de fonte aberta e estamos trabalhando com equipes de fonte aberta agora para resolver esses problemas e novamente a integração ligada com segurança.

Eu acho que o que nós temos visto que no ambiente da internet a virtualização já está acontecendo há muito tempo, então hoje há muitos serviços que fornecem serviços de internet onde se

podem mandar folks de um aplicativo para outro, podemos compartilhar o armazenamento de dados.

O que nós vimos é que não se pode garantir a segurança, imagine se alguém entrar na rede de um operador de telefonia celular. Eu sei que muitos têm problema de roaming, aqui na Índia alguns dos que chegaram tiveram esse problema e um dos problemas de roaming é que você pode ligar pra qualquer número em qualquer parte do mundo e do ponto de vista de cyber segurança é um problema e isso em termos de uma grande preocupação.

Então dentro dos padrões continuamos a desenvolver padrões do grupo ETSI NFV e estamos trabalhando junto com a GSMA que é a organização em que todos os operadores de telefonia móveis e todos os acordos de roaming ocorrem e levem em conta questões de segurança.

Então são várias áreas envolvidas aí. Então este é o último slide. Nessa apresentação há vários outros slides, mas eu gostaria de mencionar o grupo de segurança do ETSI e se vocês quiserem na próxima ISG então qualquer um pode participar, você só tem que preencher um formulário para participar.

O que nós queremos fazer é reunir os especialistas em segurança tanto da internet quanto da telefonia celular e

queremos gerar um conjunto de padrões que cheguem à comunidade de fonte aberta.

Então estamos passando de uso de chips e há muito se pode ter credenciais que podem se fazer o download de credenciais para autenticação e nós queremos fazer o melhor possível em termos de segurança, a autenticação é um problema, nós sabemos os detalhes da inscrição, não sabemos exatamente quem são, enquanto que na internet a conectividade é muito mais aberta.

Então deveríamos trabalhar juntos para que a internet seja mais segura e possamos avançar.

DAVID CONRAD: Muito obrigado Howard.

Eu gostaria de abrir o microfone aqui pra mesa ou para o público, se alguém tiver alguma pergunta para o Howard.

KUO-WEI WU: Eu gostaria de fazer um comentário dos problemas de segurança que teremos no futuro e gostaria de compartilhar algumas ideias com vocês.

À medida que esses dispositivos IoT estão se tornando cada vez mais baratos, então não gastam nenhum centavo em software. Então eles só vão à internet e buscam esse software, é mais fácil

do que vocês imaginam. Muitos dispositivos home e IoT são um problema de segurança e eu gostaria que especialmente alguns países se você tem um PC ou Mac eles são todos os software de graça, inclusive os vírus e como vocês sabem que as peças podem ser compradas muito baratas.

Eu gostaria de saber como resolver, temos que saber como fazer com que essa indústria, esses fabricantes, fazer então com que esses fabricantes atuem de forma a manter a estabilidade e a segurança de toda internet.

Esse seria o meu comentário pessoal.

HOWARD BENN: É um ponto bastante interessante.

O ETSI está trabalhando em padrões de segurança para dispositivos IoT já há alguns anos e é muito difícil garantir que os fabricantes cumpram com esses padrões e um dos grandes problemas no futuro, eu já falei em outras reuniões sobre isso, um dos aspectos que está se pensando se a internet começasse do zero agora, nós precisamos nos associar a internet, não se pode ter dispositivos sem nenhum tipo de associação com a internet, então dispositivos que causam problemas podem ser desassociados e isso é algo que nós temos que enfrentar, nós

temos que estabelecer um limite para manter a segurança e a estabilidade e impedir os ataques.

O último foi no DNS, causou problema logo de início.

KUO-WEI WU: Posso responder?

Na verdade quando o DYN, quando John Klensin mandou um e-mail pra mim há muitos anos atrás, quando a IEFT teve uma reunião no Taipei, John Klensin trabalhou muito duro para ligar os fabricantes com TI, mas isso não aconteceu porque esses dispositivos de home os fabricantes estão na China e são montados.

Então é possível conferir uma ligação, um canal de comunicação entre o IEFT e os fabricantes desses dispositivos.

PESSOA NÃO IDENTIFICADA: Nós podemos falar sobre a internet das coisas, também sobre o trabalho ETSI em Copenhague, mas eu quero convidar todos vocês a participar desta questão de tecnologia nas reuniões do IEFT.

Minha companhia é uma companhia de tecnologia mundial e nós participamos das atividades do IEFT porque nós temos orçamento suficiente e a ideia é que os fabricantes assistam as

reuniões, mas também devemos ir como indivíduos e não só como companhias, porque as contribuições do IEFT são feitas a título pessoal.

DAVID CONRAD: Jonne, você quer fazer algum comentário?

JONNE SOININEN: Não sobre isso, precisamente, mas muito obrigado.

JAY DALEY: Muito obrigado Howard, sua apresentação muito boa e você poderia falar um pouco sobre a questão da propriedade intelectual?

HOWARD BENN: Nos baseamos em uma política não discriminatória de licenças, temos debates sobre como a rede interaa com a comunidade de códigos abertos, porque muitas delas têm uma política livre de direitos de propriedade intelectual, continuamos com essas deliberações, mas fica claro que comunidade de códigos abertos e a comunidade da ETSI e outras estão trabalhando juntas para ter um trabalho frutífero.

JAY DALEY: Você mencionou no começo uma coisa que me surpreendeu, porque sobre o OpenStack e me surpreende porque há muitos países que tem muito serviços e que estão utilizando essa tecnologia OpenStack, eu gostaria de saber então se nas telecomunicações há um nível maior de envolvimento, já existe um nível maior de requerimento, esse já está requerendo com códigos?

HOWARD BENN: Não, para OpenStack não, simplesmente o grupo ETSI NFV informa a comunidade de OpenStack sobre as questões detectadas e obviamente há pessoas que são as que fazem as contribuições mas OpenStack continua a fazer a mesma política e vai continuar da mesma maneira. O único programa que realmente está sendo feito progresso é um programa aberto em que a ETSI está tentando colaborar completamente e isso está sendo tratado pela diretoria.

JONNE SOININE: Eu gostaria de mencionar uma coisa, o que Howard está tentando dizer é que ETSI tem especificações e entre essas especificações algumas visam elucidar OpesnStack ou a plataforma aberta do NFV que é uma organização que cria um marco para NFV e contribui com projetos como OpenStack.

Há companhias pelas quais eu trabalho quando não estou trabalhando na diretoria e também há companhias onde trabalham Howard e Francisco contribuem para o NFV, para o OpenStack e nós utilizamos as diretrizes consensuais na indústria e no ETSI.

A ESTI como organização e padronização é financiada pelas contribuições dos membros e Howard se referiu aqui a um grupo que se dedica a administração e organização de código aberto ou Open Source, dentro da ETSI, então eles trabalham e também trabalham com a indústria, então não se trata só dos membros desse projeto de código aberto, mas se não que esses membros estão trabalhando dentro do contexto da ETSI.

Quanto à apresentação do Howard e a história da virtualização da função da rede ou NFV, poderíamos dizer que agora há uma transição nas telecomunicações pela qual uma parte das tecnologias utilizadas antes e já há um tempo no mundo das tecnologias da informação, como por exemplo, a nuvem na virtualização e o OpenStack estão sendo também utilizados no mundo das telecomunicações e já não tem um hardware especializado e nem elementos especializados de redes, estão passando para uma arquitetura de redes mais focada em dados, uma arquitetura de dados com hardwares genéricos e softwares genéricos com algum componente privado e algum de código aberto e assim ria uma plataforma de virtualização.

Então o que antes eram elementos de redes discretas agora são máquinas virtuais ou software basicamente.

PESSOA NÃO IDENTIFICADA: Há muitas companhias de telecomunicações e operadores de cabo que fazem roteamentos e na Índia também vemos que eles estão oferecendo diferentes tipos de serviços de operadores de maneira ampla, através de caixas especiais para operar a internet, também para falar sobre questões de cyber segurança nesta região e mais uma coisa é que temos algumas questões na Índia que é um dos lugares com maior nível de reciclagem.

DAVID CONRAD: Não há mais perguntas sobre NFV?

Sim, há uma pergunta de um participantes remoto.

PARTICIPANTE REMOTO: Wolfgang Kleinwachter da Universidade de Aarhus, que diz que os fabricantes de automotores devem cumprir com padrões de fabricação e porque não se aplica isso também para os fabricantes desses hardwares e softwares?

DAVID CONRAD: Isso é interessante, eu suponho que organizações como a ETSI vão poder gerar padrões e critérios e normas regulatórias também.

Não sei se Howard quer falar sobre essa pergunta.

HOWARD BENN: Essa é uma questão perigosa, mas é também uma pergunta interessante, uma questão interessante.

Devemos demonstrar realmente que as pessoas cumpram com uma série de padrões antes de conectá-los com a internet porque essa é uma questão que estamos tratando aqui e a minha reposta agora é não.

DAVID CONRAD: Sim, é verdade, mas vemos que cada vez há mais ataques e recusas de serviço.

STEVE CROCKER: Gostaria de entender um pouco o que disse o Wolfgang, quais são os padrões internacionais existentes que devem ser cumpridos?

Eu não sei muito bem ao que se refere o Wolfgang.

DAVID CONRAD: Ele estava se referindo a indústria automotiva, para vender um carro deve cumprir com alguns requisitos.

STEVE CROCKER: Eu tinha esquecido de uma coisa, ah sim, esqueci. Um carro é muito mais avançado do que a internet, muito mais avançado. Carro não é um dispositivo da internet, não sei, mas talvez no momento sim.

JOHN LEVINE: Isso aqui é muito diferente, porque em muitos países precisamos de autorização para conduzir um veículo e acho que essa autorização vai ser na internet no final de contas.

HOWARD BENN: Então precisamos no mercado europeu cumprir determinados requisitos da comunidade europeia para poder utilizar um dispositivo móvel, isso acontece com os celulares, mas nenhum desses documentos está relacionado ao acesso à internet.

DAVID CONRAD: Vamos avançar, vamos passar então para o item seguinte.

O DNSEXTLANG, John Levine que vai falar.

JOHN LEVINE: Eu estou aqui presente e muito contente por estar aqui, vamos falar sobre essa questão aqui.

Essa é uma questão operacional um pouco diferente. O DNS, os dados do DNS consistem em registros de diferentes tipos.

Existem entre 70 e 80 tipos de dados de uso comum e sempre ouvimos falar, porque não existem novos tipos de registros ou porque não distribuímos novos tipos de dados na internet?

Frequentemente faz sentido coordenar diferentes tipos de registros, por exemplo, o Paul Wouters está procurando diferentes tipos de registros para publicar.

Podemos ver aqui na tela 4 passos para publicar esses registros, desde o cérebro até a internet. Primeiro temos os registros de DNS que devem ser guardados em um arquivo máster e historicamente as pessoas utilizavam esse arquivo com editor de texto, mas hoje vamos ao provedor de DNS registrador que tem um aplicativo na web.

É um aplicativo que não é muito bom e é por isso que nós chamamos isso de crudware ou um software cru, depois passamos isso para servidores máster do DNS que são uma espécie de DNS empodeirado, depois os registros públicos na internet e para poder utilizá-los em um aplicativo, os aplicativos tem então uma biblioteca de DNS com registros que vão para os

arquivos em cachê que tiram esses dados do arquivo master. É dessa maneira que estamos funcionando por muito tempo.

Agora na hora de definir novos tipos de registro o que acontece é que o IETF publicou um documento RFC que define esse tipo de registro sobre a sobreposição da implementação e da publicação, então primeiramente deve ser atualizada a biblioteca, então quem manter a biblioteca deve adicionar esse novo tipo de registro, utilizar a distribuição para que todos possam utilizar a biblioteca para que todos possam utilizar o software e isso pode ser feito.

Também é atualizado um software master para que inclua esse tipo e registro. Esse não costuma ser um problema porque as pessoas encarregadas dos servidores DNS atualizam isso bem rapidamente, distribuem versão que as pessoas podem instalar ou não e o crudware raramente é atualizado e, portanto podemos utilizar os mesmos tipos de registros que eram utilizados antes.

O objetivo é que cada vez que um novo tipo de registro é definido esses 3 componentes possam ser atualizados automaticamente e isso significa que os servidores master e software da biblioteca possam entender a sintaxe do novo registro que será o nome do novo tipo de RR e devem entender o

formato binário, traduzir o texto em formato binário e vice-versa e o software master e a biblioteca devem ter essa capacidade.

Como isso está na web devemos direcionar as pessoas a sintaxes necessárias. Então aqui deveríamos ter uma linguagem que permita descrição dos tipos de registro, nós mencionamos que os colocávamos em arquivos de teste, mas por fim se teve a ideia de publicar a descrição no DNS e o sistema automaticamente pode encontrá-la e uma vez feito isso atualizamos o software para que possa trabalhar com essa nova linguagem e temos uma atualização automática dos registros, aqui temos uma descrição de alguns registros, um mail exchanger, um é registro MX que é bastante comum e aqui temos alguns registros de campos com arquivos de texto.

Então nessa descrição na primeira linha nós temos o registro de SRV bastante complicado, o nome é SRV e o tipo é 33, o I significa - os DNS têm classes. Então isso deve ser usado pelo usuário e o segundo é o peso, terceiro é a porta e é o nome de domínio que o alvo e o target e há descrições de todos os tipos de registros nessa norma e para lidar com quase todos os tipos novos de registros há 14. Há 3 tamanhos de cadeias de textos, domínios, endereços de v6 e v4, todos os tipos de outras coisas como horários, hashes de 32 e 64 bits, etc e há um tipo chamado “Z” que não pode ser descrito em um tipo de evento que não pode ser descrito pelos outros registros e nas inscrições dos

tipos de DNS há opções e as opções que eu coloco são 3, aqui é o registro NSEC3, o primeiro campo, o algoritmo, pode ser definido como um número ou pode ser mnemonic, então se o tipo de usuário é isso e o segundo é um flag, podem ser múltiplos campos. Alguns campos têm vários tipos, mas no terceiro campo é um campo hex que armazena a conta e o último são os tipos, alguns registros são tipos de registros, nesse caso são tipos de registros armazenados nesse tipo de nome.

Então no NSEC vários tipos, há uma lista. Vocês podem olhar o texto para ver as diferenças, o que eu quero mostrar é que as opções de campo não são complicadas.

Se olharmos o RFC que define, nós podemos ver como deve ser feito e isso pode ser descrito facilmente. Poderia voltar ao outro slide?

Essa descrição da informação suficiente de que os registradores mestre e que as bibliotecas podem classificar os registros, pode interagir com o campo hex e dar uma lista de tipos e com essa descrição se pode, ou isto é suficiente para que possa classificar os registros mestres e os binários.

Então para um usuário que vai definir um registro MX então ele vai digitar o MX e vai aparecer esse formulário e há uma prioridade e o host name na descrição e o usuário então digitou 100 e o nome do servidor e o usuário precisa conhecer um

pouco o que quer fazer, ou saber o que quer fazer, mas o que ele faz é mostrar facilmente o que você tem que digitar, então é bastante fácil e nós temos que obter os dados do DNS, então Paul teve a ideia de publicar as descrições dos registros que estão no DNS.

Podemos procurar por número ou por nome, aqui temos um registro hipotético como 999, aqui temos a descrição, 999.RRTYPE.ARPA e tem um texto comum do DNS de forma que se possa conhecer a sua disponibilidade, tem a sigla EN, se podem escrever diferentes versões para internacionalizar os registros em idiomas locais e termos a cadeia como eu demonstrei a descrição dos nomes e os nomes de registros individuais então é fácil escrever um software dessa maneira, então com isso definimos um novo tipo de registro e o que nós fazemos depois publicar o RFC com a descrição e isso é colocado no DNS e o software que utiliza isso pode buscá-lo.

Isso não é uma panaceia universal para todos os registros, há alguns tipos RRTYPE que são difíceis de contar que tem a ver com a ordem dos campos e a ordem dos campos que não coincidentes, é preciso escrever um código para interpretá-las, mas em geral todos esses tipos são gerenciados por servidores especiais e não são tipos que o usuário em geral não quer utilizar, porque serão obsoletos como o caso do antecessor do DNSSEC e o servidor precisa de funcionalidades especiais, como

por exemplo, quando se quer encontrar as versões do NSEC, há versões anteriores que não são necessárias.

Eu posso escrever a sintaxe dos registros, mas não posso dizer qual é o cachê, então tivemos que inventar a DNSSEC apenas uma vez e as alterações que demandam semântica se fazem a cada 2 anos e isso não nos preocupa.

Depois de ter inventado isso nós começamos a implementar e o David Conrad deu apoio a implementação. Então a minuta da especificação já está feita, eu modifiquei a biblioteca DNS perl, então pode-se ler diferentes tipos de arquivos, registrar os tipos de registro DNS, então se pode automaticamente rapidamente ver o tipo de registro e é bem fácil e podemos então falar como integrar melhor o DNS, ou a distribuição padrão na biblioteca e isso é gratuito, de fonte aberta, esperamos que uma vez feito isso adicionar novos tipos de registro será mais fácil e as pessoas estarão mais dispostas a fazê-lo.

Tivemos poucos tipos novos de registros, porque se acha que se é um novo tipo de registro ninguém vai usar porque o provedor não consegue lidar com isso, então muitos serviços utilizaram registros de texto e na maioria dos casos isso funciona.

Então é assim que o software funciona e espero que sejam usados.

STEVE CROCKER: Muito legal ter trabalhado pelo emprego do DNSSEC e os problemas dos novos tipos de registros, qual é a aceitação e alguns problemas que ainda não foram resolvidos. O que mais precisa ser resolvido, eu entendo esse problema.

Eu tenho algumas perguntas sobre o protótipo.

Então olhando um pouco para o futuro, 2 tipos de perguntas que estão ligadas, tem a ver com sucesso e fracasso. Então os novos tipos de registros que foi definido e seus novos usos que agora torna popular o DNS e há resolvedores que estão buscando esse novo tipo. Existem 2 gargalos possíveis.

Um de todos usarem ao mesmo tempo o mesmo lugar e se isso não for levado em conta o .ARPA vai cair e quanto tempo demora para trabalhar um resolvedor que tenha uma carga considerável para absorver, reconfigurar e responder?

A outra pergunta é, eu vejo que isso foi motivado para resolver os problemas que já havia, então e quanto a novos tipos de registros.

JOHN LEVINE: Em resposta a primeira pergunta quanto ao desempenho eu não tenho a menor ideia, vai depender da estratégia de cachê, então

e se eu tiver um servidor muito ocupado e uma biblioteca compartilhada eu acho que é uma questão de detalhes de qualidade de implementação.

Há alguns tipos novos de registros que estão surgindo e, como o meu, que podem ser descritos facilmente como bom, vai funcionar bem se esses novos registros usarem os campos que usávamos antes e depois de fazer o inventário de todos os registros feitos e tentando definir, as pessoas têm usado tipos de campos reutilizados.

Houve um novo para EU48 e EU64 para endereços Mac e parece funcionar muito bem, parece ser uma questão de quem veio antes, a galinha ou ovo? Então se as pessoas acharem mais fácil de implementar um registro vai ser fácil de ter um campo de descrição de tipo.

PAUL WOUTERS: Eu gostaria de fazer um comentário, na verdade não se tem que fazer um trabalho novo, os resolvedores não tem que fazer mais trabalho porque eles estão fazendo ligados ao DNS, então para obter novos tipos de registro a questão é quando um humano quer fazer isso. Então para que isso não aumente a carga do servidor.

JOHN LEVINE: Bom isso não é bem assim.

As aplicações precisam escrever parte do registro, então se eu quiser escrever um aplicativo meu aplicativo precisa saber, bom aqui é o hash, aqui estão os dados.

PAUL WOUTERS: Então o aplicativo precisa saber quais são os campos, então se você está fazendo isso é um problema, porque isso é parte do DNS e isso pode ser um grande problema, pode ser assustador na verdade.

JAY DALEY: Eu sei que alguém tentou fazer algo semelhante que foi um fraudador com os tipos de esquema de DNS e descreveu o DNS muito bem e fez as divisões dos campos. Como será internacionalizado isso para o usuário final?

JOHN LEVINE: Bom, os registros individuais, um deles a única coisa que vai precisar de transação é uma cadeia de campo para usuários finais.

Os endereços I.P. sim é um pergunta muito interessante, é um tópico que ninguém pensou nisso antes, as cadeias e os textos hiperlimpos e ninguém presta muita atenção nisso, então se nós

pudéssemos imaginar em níveo do IEFT que queremos armazenar dados de texto que não estiverem no ASCII no DNS devemos seguir como decidir isso.

JAY DALEY: Sim, é isso que eu queria dizer, atualmente como aparecem os nomes? Não aparecem no DNS, então se alguém apresentar esses nomes a outro que vai procurar em outra parte vamos ter uma questão de escolha de língua e vamos precisar de uma versão de língua declarada de cada uma.

JOHN LEVINE: Na versão do DNS há um rótulo de linguagem, um tag no registro de DNS tudo bem, mas isso é extremamente longo, mas outro aspecto é o aspecto to EPP, o EPP no centro tem modelo de dados definido muito fixo e eu conheço alguém que sugeriu que o EPP deve especificar ou conter um mecanismo pelo qual os novos dados, em vez de incluir os dados, devem escrever os dados que vão receber, então para que as pessoas nos diferentes registros adicionem alguma coisa como endereço deverão fazer isso através de uma inscrição, mas se o EPP estiver em um nível mais descritivo isso seria bem melhor.

JAY DALEY: Você sugere então que essas duas coisas poderiam se unir de maneira positiva para o usuário?

JOHN LEVINE: Sim.

JAY DALEY: Porque então teremos novos registros que deverão ser codificados dentro do EPP para eles poderem ser transferíveis entre as partes.

Existe alguma vinculação?

JOHN LEVINE: Sim, os conceitos são similares, não sei quanta semelhança haverá na hora de implementar isso.

DAVID CONRAD: Última pergunta.

WES HARDAKER: São ideias interessantes.

Primeiramente algumas recomendações ou pedidos. Primeiro não pôr o formato de internacionalização no registro porque há muitos e porque não colocar um tag?

JOHN LEVINE: Sim, eu pensei nisso, mas o problema é duplo.

Primeiramente como fazer o valor de fold, isso pode ser feito com asteriscos, mas não ficaria bem, seria complicado e além disso se nós quisermos fazer isso corretamente o exemplo a seguir é o código em 2 línguas, em inglês são 2 códigos de línguas, EN para o inglês e isso é trivial no banco de dados e não tem possibilidade de fazer isso no DNS.

WES HARDAKER: Seria impossível com um pacote muito grande.

JOHN LEVINE: Sim.

Outra possibilidade é por o tag da língua no nome.

WES HARDAKER: Não se esqueçam que os formatos de visualização do formato mais recente se afastam dos bits e se dirigem a palavras individuais, como a palavra DANE e que se atualiza agora em vez de escolher ser 1, 2 e 3 colocam palavras chave reais que se correspondem certamente.

Algo interessante são as ramificações interessantes de planejamento, por exemplo, quando alguém falsifica um registro e diz que os campos são invertidos e faz com que o usuário coloque dados na sua zona e me pergunto se aqui não entra em jogo questões de segurança.

JOHN LEVINE: Estamos a mercê de pessoas que mantém as descrições, mas temos o mesmo problema quando as bibliotecas são atualizadas.

WES HARDAKER: Se eu posso falsificar os dados .ARPA, então posso trabalhar com qualquer aplicativo que potencialmente pode causar o ingresso de coisas diferentes.

JOHN LEVINE: Sim.

WES HARDAKER: Como mudar o password.

STEVE CROCKER: Sim.

Se publicarmos uma descrição e depois precisamos editá-la e fazemos um erro então aí deveríamos altera a palavra chave para evitar um acionamento da atualização da palavra em toda rede, ou então ser utilizada a palavra antiga o tempo todo.

JOHN LEVINE: Não pensei nisso, mas é muito estranho que seja atualizado isso no RFC por um erro de alguém, é necessário excluir um mesmo nível de cuidado, não podemos errar dessa maneira.

STEVE CROCKER: Mas a internet é isso mesmo.

JOHN LEVINE: Podemos falar de tags de versão ou timeout, mas gostaria de tentar resolver esse problema antes de nada, porque isso complica as coisas.

DAVID CONRAD: Jay.

JAY DALEY: Não fica claro porque isso deve estar no DNS e que relação isso tem com essa situação de ter que cobrir novos RRs e TTLs para que isso seja um sítio operacional tem que ser ativo, não pode

ser estático, não entendo porque esperar que um software procure a cada 2 ou 3 horas, eu não entendo. A implementação que eu tenho aqui vai procurar cada vez que for encontrar um registro e depois isso é coleto e é guardado na caixa local.

Então quando encontramos algo que não conhece e o procura.

JOHN LEVINE: Sim.

DAVID CONRAD: Paul, você queria fazer um comentário?

Então muito obrigado John.

Então agora vamos passar a Warren Kumari que vai falar sobre o trabalho que está sendo feito no IEFT.

WARREN KUMARI: Eu e Paul somos representantes do IEFT, quero comentar o que estamos fazendo.

Nós somos contato entre a IEFT e o TEG. Vou pular a primeira apresentação e dependendo to tempo restante vou voltar a ela ou vou apresentar outro conjunto de slides.

A sinalização do KSK, qual é o problema? Há dada regulamentação, mas infelizmente vocês vão receber a nova

senha e um RFC denominado 5011 e alguns servidores de nomes não suportam o RFC 5011 e que decidiram não implementá-lo, a maioria das implementações suportam, mas muitos tem isso desabilitado e isso é quando começamos a introduzir o DNSSEC e fizemos apresentações em workshops, etc, houve alguns exemplos que incluíam uma configuração que dizia que essa era a senha e que não devia ser alterada.

Então muitos acreditaram que essa era a chave da raiz decidiram não alterá-la. As pessoas gostam dos diagramas e esse diagrama mostrava os resolvedores, alguns suportavam o RFC 5011 e outros os tinham estabilizado, não havia uma maneira de medir os tamanhos de círculos no diagrama, não temos como contar quantos deles fazem 5011, então esse é aqui um fragmento do plano de lançamento do KSK, é o que eu digo basicamente que medir é difícil, mas aqui temos um documento que pode ajudar-nos nesse sentido.

Eu acho que o título é aqui gestão do gerenciamento do KSK que diz basicamente o seguinte, diz que os resolvedores quando fazem novamente o processamento do RFC 5011 enviam uma consulta que inclui uma lista das âncoras confiáveis e então nesse exemplo tem uma âncora confiável que se chama 1984 que passa para a 4242, o consultor então envia consultas procurando o ta-1984 e consultas que tenham o 1984-4242,

então quando essa fileira é completada enviam mais consultam que contém ta-4242.

Isso permite que alguém que está observando o tráfego na zona raiz possa observar e ver a porcentagem dos usuários que tem a senha antiga e quais tem a senha nova.

A mesma informação também está codificada de maneira diferente e colada a uma opção ENDS, mas o que é interessante aqui antes de completar a transferência é quem é que pode quebrar ou violar isso e quem pode resolver isso e se existe alguma solução para o problema, mas não é uma solução completa.

Se instalações prévias ao suporte RFC 5011 por definição surgiram antes da publicação desse documento, isso significa que ainda temos uma porcentagem de usuários importantes.

Então no IEFT em breve vai ser publicado um documento, um grupo de trabalho que já acabou seu trabalho vai passar um pouco de tempo antes que o pessoal implemente um código resolver e que depois seja feito o desdobramento, então devemos esperar que para a próxima transferência da KSK, independente de quanto tempo existam estatística úteis.

Então qual é a solução aqui?

STEVE CROCKER: Eu quero falar sobre uma coisa que está diretamente relacionada.

Quanto a sinalização das chaves isso é comparável a sinalizar os diferentes tipos de algoritmos e você disse que sim, então há uma certa coordenação sobre o mecanismo que deve ser utilizado e então talvez isso seja um assunto para outro diálogo e não sabemos muito bem onde estão esses resolvedores e isso se assimila a algo que nós já conversamos há algum tempo sobre todos os tipos de dispositivos conectados a internet e dos quais não sabemos qual é a situação quanto a segurança, poderíamos pensar em registrar todos esses dispositivos na rede, mas é uma questão que nos preocupa porque é uma tarefa muito importante e devemos ver como registrar da mesma maneira todos os resolvedores do DNS na internet para contatá-los e ver o que acontece caso haja alguma situação que deva ser resolvida.

WARREN KUMARI: Sim, falamos em incluir a versão dos resolvedores, mas decidimos publicar isso primeiro e depois ter um documento com os algoritmos.

JAY DALEY: Desculpem se eu continuo aqui pedindo a palavra, mas há muitas cosias que não sabemos sobre os resolvedores e digo isso olhando para o David e devemos trabalhar sobre isso para vermos que resolveredores fazem que coisas e também devemos trabalhar sobre outras coisas importante, talvez devamos tentar novamente fazer um acompanhamento de todos esses resolvedores e se nós tivermos sondagens corretas também teremos as estatísticas corretas para transferir os resultados.

DAVID CONRAD: Sim, a minha equipe está tentando junto com Paul Hoffman de pesquisar sobre a implementação do resolvedor e estamos tentando ver esses dados analíticos, os dados do DNS e publicar a demografia disso.

JAY DALEY: Muito bom.

Acho importante incluir esses detalhes.

RON da SILVA: Quanto aos dados analíticos sobre os resolvedores, me parece algo excelente, eu gostaria de saber quais são os passos pró-ativos de comunicação que estão sendo feitos para chegar as

pessoas que utilizam diferentes resolvedores? Eu sei que há uma grande lacuna e não sabemos o que vai acontecer, o que estão fazendo pró-ativamente?

DAVID CONRAD: Com relação a transferência da KSK nós temos um plano de comunicação bastante completo, está publicado no site da ICANN, na implementação. O que nós estamos fazendo agora é como ter acesso aos dados de consulta ao servidor raiz. Estamos vendo as fontes das consultas em termos de endereço de I.P. e nós sabemos que há muitas informações desnecessárias no servidor raiz e fazemos uma busca reversa para ver quem está buscando esse resolvedor para dizer que algo vai acontecer daqui há 1 ano e estamos tentando ver se o resolvedor do DNSSEC o que torna mais interessante. Isso que estamos fazendo em termos de pesquisa.

DANIEL DARDAILLER: Vocês tem alguma restrição em relação a quem pode solicitar o KSK do resolvedor?

WARREN KUMARI: O que nós fazemos é publicar isso da raiz em relação a consulta de forma que ela tenha uma cadeia de caracteres completa, é

isso que nós estamos fazendo como ponto de ancoragem de confiança nos servidores raiz.

JAAP AKKERHUIS: Na semana passada foi dito que há um mapa de 95% dos resolvedores ativos, Geoff e Joel tem essa informação.

Eu falo com eles às vezes.

DAVID CONRAD: Há alguma pergunta sobre essa questão, senão eu acho que nós podemos passar para outra apresentação de Warren Kumari e passamos então para a próxima apresentação.

WARREN KUMARI: Temos uma outra apresentação, inicialmente essa apresentação ia demorar meia hora, mas eu só tenho 15 minutos, então eu vou tentar apresentar o conteúdo, vou falar rapidamente.

O DNSSEC tem autenticações de respostas positivas e negativas, então procuramos um site e temos o indício que isso é correto e também faz a autenticação de respostas negativas, então se procuramos um nome inexistente o DNSSEC indica que o nome não existe e há uma assinatura que demonstra isso.

Gerar assinaturas é uma operação bastante cara, então no DNSSEC se evita isso, por isso nós temos o NSEC, next secure,

que o que faz é procurar todos os textos, classificar alfabeticamente e assinar os espaços entre os textos e não precisamos saber qual é a pergunta específica.

Isso é algo confuso, por exemplo, aqui temos uma busca para o site em especial, uma cadeia de caracteres muito comum, esse é um TLD inexistente, então nós temos esta busca e eu faço a busca e é indicado que o domínio não existe e eu tenho o registro NSEC que não há nada que exista entre este e outro domínio e aí eu tenho uma série de criptografia que demonstra que isso de fato é verdade e vejo assinatura que comprova isso, isso é interessante, qual é a utilidade?

Esse documento do IETF mostra que os resolvedores recorrem depois de utilizar a informação nos registros NSEC para sintetizar as respostas, por exemplo, se tivermos uma busca de um domínio que está entre outros 2 domínios nós temos uma busca específica para o domínio correspondente e o documento diz que não é necessário realizar isso porque se já há um registro NSEC que o número não existe isso pode ser utilizado e respondido imediatamente.

Isso melhora a privacidade do usuário, porque os nomes que não existem não são filtrados na internet e o resolvedor pode responder imediatamente a menor latência e não é enviado um

conjunto de consulta, então nós temos uma funcionalidade que melhora a resiliência.

Os hackers utilizam vários nomes inexistentes, consultam ao servidor que tem autoridade e se isso for feito várias vezes há uma sobrecarga do servidor, então se há um servidor recorrente que faz uma sobrecarga no servidor não é uma resposta, então isso é útil?

Temos exemplo do dia 12 de maio que foi uma sexta a tarde no qual temos o pessoal do RIPE que enviou uma consulta dizendo que havia consultas indesejadas pelo Google mostradas aqui que parecem cadeias de caracteres aleatórios e me pediram que isso fosse retirado, eu não sei se podem ver bem o gráfico na tela, mas vemos que quando começou a aumentar a quantidade de consultas, eu trabalho no Google e começamos a ver o DNS público do Google para ver qual era a razão, se alguém estava modificando códigos, se havia algum tipo de efeito, se isso era um ataque ao DoS e o que foi bastante alarmante porque parecia haver um crescimento. Porque um ataque de delegação de serviços sempre começa em uma determinada veracidade e depois para, então continuamos pesquisando não era apenas o DNS público do Google que estava enviando, mas vinha também de outros resolvedores, então que bom que não éramos os únicos, continuamos pesquisando e vimos que havia um worm novo que estava afetando os pontos de acesso e também em

roteadores que continuavam a infecção das máquinas que buscavam uma cadeia de caracteres específicas para chegar na internet e a cadeia de caracteres era aleatória com um conjunto de objetos aleatórios também, bem agora sabemos que a culpa não era nossa, mas o que podíamos fazer?

Aqui temos um gráfico com consultas do DNS público do Google aos servidores do raiz B que tem uma entidade operacional específica, não sei se vocês conseguem ver os números, mas a esquerda vemos que antes do ataque esse servidor raiz recebia do Google 500 consultas por segundo e a partir de então houve um pico de crescimento e o DNS público o Google tinha esse software, mas não estava habilitado, ele foi habilitado nos 4 principais locais, então 100%, foi sexta-feira. Então não fizemos mudanças de produção e na segunda-feira continuamos essa tarefa em todos os locais e deixamos rodar por uma semana e vemos a direita que em 100% foram habilitados em todos os locais.

Então a direita vemos que a quantidade de consultas diminuiu para 30 a 40 consultas por segundo. Bom, o que está no documento? Em parte o que eu já mencionei, se nós tivermos um registro NSEC que demonstra a existência de um domínio nós não nos preocupamos com isso, mas se tem um registro wildcard não precisamos procurar e enviamos a resposta imediatamente e com isso eu termino a minha apresentação.

Atualmente a raiz tem 60% de consultas que são resolvidas indicando a inexistência do nome de domínio, mas essas consultas inválidas poderiam diminuir a 1% se todos aplicassem essas técnicas que eu descrevi.

Desculpem se eu falei muito rápido e agora eu vou responder as suas perguntas.

DAVID CONRAD: Alguém tem alguma pergunta para o Warren?

WARREN KUMARI: Isso funciona com NSEC3 também, nesse caso o NSEC3 funciona quase igual ao NSEC, mas devem-se classificar os nomes existentes e devem ser classificados todos os hash.

DAVID CONRAD: Há alguma outra pergunta?

RAM MOHAN: Warren, o nível técnico é tão detalhado que os outros colegas estão perdidos depois da sua apresentação, então você poderia resumir o problema, poderia ajudar.

WARREN KUMARI: Desculpem, eu falei muito rápido.

O resumo é que se forem implementadas essas medidas vai diminuir a quantidade de consultas em várias raiz e em outros domínios, aumenta a privacidade do usuário, o desempenho e reduz a quantidade de buscas que chegam aos servidores autoritativos, então eu posso falar mais devagar se precisarem de mais detalhes.

WES HARDAKER: Eu gostaria de agradecer pela apresentação, você evitou que os meus dispositivos móveis parassem de funcionar esses dias.

JAY DALEY: Eu acho que não foi esclarecido muito a questão do desenvolvimento dos resolvedores ao longo dos anos e se houvessem mais dados na indústria alguns problemas teriam sido resolvidos e medidas de proteção teriam sido implementadas e alguns problemas teriam sido solucionados

RAM MOHAN: Muito obrigado, eu quero pedir que membros da diretoria falem.

DAVID CONRAD: Há alguma outra pergunta?

JOHN LEVINE: Isso já foi implementado?

WARREN KUMARI: Eu sei que em alguns dos lugares o DNS do Google faz isso e eu acho que é uma das plataformas padrão.

DAVID CONRAD: Bem, muito obrigado. Então nós podemos passar para qualquer outro tema. Alguém do TEG ou no público gostaria de falar?

YOSHIRO YONEYA: Houve uma pergunta, como aplicar o BCP38. Essas partículas spoofed ou pacotes spoofed foram usados para esses ataques, então empregar o BCP38 é muito importante para reduzir esses ataques, eu acho que aqui é um bom lugar para falar disso.

Então eu sei que é uma questão de prática operacional, mas temos que explicar que o IEFT e a ICANN também expliquem isso.

DAVID CONRAD: Eu sei que o SSAC publicou alguns documentos sobre a utilidade do BCP38, mas isso foi importante que o SSAC reitere a utilidade do BCP38, mas não é algo que o TEG queira se concentrar nisso.

Ram, você quer dizer alguma coisa?

RAM MOHAN: Então eu vou te botar o meu chapéu da diretoria e tirar o de técnico.

Então em relação ao feedback para o TEG. Deve haver algumas coisas que nós devemos pensar em fazer para que haja um diálogo melhor, uma sugestão é de que quando a agenda for feita tenhamos algum tipo de resumo executivo de alto nível que explique quais são os problemas, porque isso é importante e porque vocês se preocupariam com isso.

Porque isso é uma coisa importante que está faltando, porque nós do lado técnico nós lemos o tópico e sabemos por que devemos os preocupar, às vezes eu acho que alguns tópicos que estamos lidando é ótimo para alguém dizer.

Bom, isso é uma coisa de técnicos, deixa que esses técnicos trabalhem nisso, isso é um feedback e em segundo lugar, na fase de reunir a agenda ou elaborar a agenda eu acho que é importante pedir contribuições da diretoria, especialmente de quem não é técnico de ver qual é o tipo de tema que eles estejam interessados.

Eu acho que isso será muito útil e a última coisa é que há uma necessidade urgente de algum tipo de inserção tutorial que talvez usando vídeos e que estejam disponíveis não só para

aquela sessão em especial, mas dali a diante para que se torne um tipo de biblioteca de informações, não só para a diretoria, mas para o resto da comunidade de tópicos importantes, muitas vezes o pessoal da comunidade me diz, bom na ICANN vocês só elaboram políticas e recomendações, mas nós estamos também fazendo tarefas técnicas e muitas dessas coisas são inacessíveis para muitos que estão nessa reunião.

WARREN KUMARI: Muito obrigado, é muito útil o seu comentário. O objetivo desse grupo de trabalho e especialistas técnicos é justamente ser um contato com a diretoria, com os membros da diretoria com conhecimentos técnicos, então poderíamos ter esses tutoriais, a questão do BCP38 e talvez a diretoria gostaria de resolver informações sobre essa questão ou talvez deseje mais informações sobre outros temas técnicos.

Podemos fazer mini-tutoriais, ter uma sala grande de reuniões para essas sessões, mas estamos abertos a ouvir sugestões para que vocês da diretoria possam processá-los melhor.

DAVID CONRAD: Claramente há interesse em receber esses tutoriais. Nós tivemos uma série de tutoriais, denominamos how it works e nós a comunidade e aos participantes e talvez possamos alongar

essas iniciativas se a diretoria tiver interesse em receber esses tutoriais, a minha equipe vai participar sim nesse caso e também se tivermos recursos técnicos para fazer isso, quanto aos temas da sessão foi muito difícil encontrar temas para tratar na sessão desse grupo.

Eu consultei com membros da diretoria, com um grupo de especialistas e por enquanto esses grupos não tem funcionado para criar um cenário, então estou aberto a receber comentários e sugestões sobre as questões e os tópicos de questões específicas porque esse grupo foi criado especificamente para oferecer informações a vocês. Nós, os técnicos, sempre falamos em títulos nós em diversos espaços, então com muito prazer vamos receber suas contribuições.

Ram.

RAM MOHAN: David, por exemplo, há algumas semanas houve a publicação de relatórios de redes em diferentes, na mídia e na diretoria surgiram perguntas não apenas do relatório e o que ele significa, como lê-lo, isso é, nós precisamos que nos ajudem a analisar e interpretar diferente assuntos.

WARREN KUMARI: Sim, claramente os membros da diretoria e dedicar 2 horas com algo que não é valioso não é útil, então, por favor, digamos se vocês não estão interessados, se isso é excessivamente técnico.

MAARTEN BOTTERMAN: Muito obrigado.

Eu vim aqui porque isso está estritamente relacionado com nossa missão, é por isso que eu quero aproveitar essa reunião, no começo eu achei que eu poderia entender o que vocês fazem, mas se a intenção de vocês é informar a pessoas como eu, eu vou precisar desse tutorial, isso simplificaria muito as coisas e segundo eu pediria que as apresentações sejam feitas em um nível que as pessoas que estiverem interessadas e querem conhecer um pouco sobre a questão pudessem participar. Muito obrigado pelo que vocês tentaram fazer.

STEVE CROCKER: Concordo com todos os comentários sobre os ajustes, mas eu queria indicar que dentro do contexto dessa participação eu acho que os comentários feitos até agora foram muito valiosos e isso nos dá uma exibição muito diferente, com o que tem a ver com as questões técnica em primeiro lugar e eu aloco um papel muito importante a conscientização e a informar sobre detalhes, estou muito satisfeito e eu quero que isso fique bem

claro, isso não é uma crítica, eu entendo que é um processo muito valioso esse que temos aqui, pode evoluir e melhorar com o tempo, mas como ponto de início estou contente.

PATRIK FALTSTROM: Obrigado para os membros do TEG e SSAC e que queria esclarecer uma coisa.

RAM MOHAN: Patrik, não é que essa questão seja muito técnica ou que deveria ser menos técnica, deveríamos pensar porque nós estamos aqui, porque essa questão é importante e depois entrar no assunto, isso é dar um contexto.

CHERINE CHALABY: Eu gostei muito dessa sessão, especialmente o primeiro e último assuntos.

Eu os achei úteis do ponto de vista do contexto, mas o que não fica claro é a questão de que a TEG se reúna com a diretoria, acho que vocês estão se reunindo com um subgrupo da diretoria, aqueles que entendem mais do assunto, mas se nós quisermos que todos participem, os membros da diretora, acho que deveríamos enviar materiais antecipadamente para que o pessoal se prepare e talvez aumente o nível de participação.

Devemos determinar o que nós queremos obter desse nível de interação, não fica muito claro pra mim agora.

STEVE CROCKER: Quantos membros da diretoria estão envolvidos?

Quanto à abordagem básica eu assumo, sobretudo na interação com o David e a equipe de especialistas técnicos quer interagir com a diretoria e, por outra parte, a diretoria, como você e eu sabemos bem, tem uma agenda muito completa e não fizemos ainda um requerimento formal a todos os membros da diretoria para marcar essas reuniões, então nós temos aqui uma quantidade importante de membros da diretoria e isso tem a ver com como a diretoria trabalha. Nem todos fazemos de tudo. É uma versão ad hoc dessa abordagem de auto-seleção e eu fiz a contagem dos membros e inclusive Göran, a questão aqui temos aqui 10 membros da diretoria e na diretoria somos 20, inclusive as pessoas contato e bom, é mais da metade.

Isso tem um efeito positivo. Então eu acho muito bem, acho que não fracassou a assistência a essa sessão, mas o importante de expressar é que assim como você, os técnicos se sintam a vontade com as apresentações e sempre podemos fazer ajustes no processo ao longo do tempo, mas como disse antes estou muito satisfeito com o nível de participação e com o efeito que ele tem e claro sempre pode ser ajustado.

CHERINE CHALABY: Gostaria de responder rapidamente, obrigado Steve pelo esclarecimento.

Seria interessante ver o que opina o tag de interação com a diretoria, é importante conhecer essa evolução.

WARREN KUMARI: Uma última coisa, eu sei que vocês estão muito ocupados, mas por favor, deixem um tempo para revisar o que seria mais útil para vocês, que nós poderiam dar para vocês.

CHERINE CHALABY: Isso foi muito útil e vamos tentar com que isso seja mais útil no futuro.

DAVID CONRAD: Ainda faltam 8 minutos para o recesso, agradeço aqui vamos ter uma recepção no Casbah, no hotel Westin, temos 2 ônibus, um que vai sair daqui há 7 minutos e outro que vai sair as 7:15, a reunião começa as 7:30 e vai até 9:30 e vamos tomar uns drinques.

7 e 7:30 são os ônibus, espero vê-los lá e se for assim vou beber todos os drinques que vocês não beberem.