ABU DHABI – Encontro conjunto: Diretoria da ICANN e TEG (Grupo de Especialistas Técnicos)
Quarta-feira, 1 de novembro de 2017 – 17h00 a 18h30 GST
ICANN60 | Abu Dhabi, Emirados Árabes Unidos

DAVID CONRAD: Eu gostaria de convidar os outros membros da diretoria para vir a mesa, nós temos alguns espaços vazios, há lugar aqui para outros membros da diretoria, se vocês quiserem sentar aqui na mesa. Muito obrigado, Marcus e Becky.

Muito bem, podemos começar. Bem-vindos a essa reunião do grupo de especialistas técnicos. São vários especialistas técnicos se reunindo com a diretoria da ICANN e esse temos uma coisa nova que com a criação do comitê técnico da diretoria, eu acho que essa é uma reunião obrigatória, eles não podem deixar de comparecer, mesmo que quisessem. Então, por uma questão de tempo, eu vou fazer uns comentários muito curtos, mas eu quero dizer que eu estou usando uma gravata hoje e não é porque eu vou dar entrevista, mas em honra do Steve Crocker que será a sua última reunião com o TGI.

Eu gostaria de dizer a título pessoal que agradeço todo o trabalho que o Steve fez, especialmente a criação desse grupo e foi criado o cargo do CTO e caiu no meu colo, então muito obrigado Steve, pelos esforços que fez para melhorar a posição técnica dessa

organização e me ajudar como CTO e várias outras coisas. Com isso, você quer dizer alguma coisa?

STEVE CROCKER: Muito obrigado por suas palavras, você trabalhou muito, fez muita diferença e a boa notícia é que você ainda está aqui no grupo de especialistas técnicos. Eu fico muito satisfeito, isso surgiu de forma inesperada, mas acho que agregou uma fonte de especialização, insight criatividade; um lugar para certas discussões que talvez não acontece se não tivesse esse grupo.

Acho que esse grupo foi criado e tem bastante vitalidade. Eu espero ter ajudado e agora burocratizado e não pode ser mais desfeito e o David tomou para si os aspectos administrativos e a elaboração da agenda. Foi ótimo.

DAVID CONRAD: Podemos começar com o conteúdo, a primeira apresentação é pelo Fernando Lopez sobre identificadores persistentes no DNS, é uma demonstração, um protótipo, uma prova de conceito que usa identificadores persistentes que são semelhantes ao que é descrito ao que é chamado de DOA, ou que seja, arquitetura dos objetos digitais.

Essa apresentação será feita em espanhol, então se você não falar em espanhol os interpretes vão ajuda-los. O Alain que dizer algo.

ALAIN DURAND: Eu vou apresentar os primeiros slides que levam a demonstração. Eu vou falar em inglês.

DAVID CONRAD: A sua versão de inglês, você quer dizer?

ALAIN DURAND: Bom, eu posso falar em francês, mas eu acho que você não vai entender. Primeiro slide é um documento de informações, mas eu pediria que mudassem para os slides.

Bem, eu vou começar com algumas declarações de isenção de responsabilidade. Esse trabalho começou no escritório do CTO e o objeto era ver se esses identificadores persistentes, semelhantes aos da DOA poderiam simplesmente ser atingidos através do DNS. Esse trabalho foi feito junto com a Universidade de La Plata, que o Fernando vai falar.

Isso não é do endosso da tecnologia do DOA pela ICANN e no contexto de persistência, foi alegado que os URL podem ser interrompidos por várias razões: alterações organizacionais,

nomes de empresas, fusões e aquisições. Isso pode resultar em falha em várias soluções disponíveis. A solução para o DOA é para ter essa solução para lidar com prefixos que usam números. Os nomes são tem uma semântica e se a organização muda, o nome pode permanecer.

Você pode mudar a organização, levar o nome com números, isso não tem problema. O lado do sufixo, em vez de ter uma estrutura profunda, que é refletida na estrutura interna da Companhia, há um espaço bastante simples, sem hierarquia. Parece que esses protocolos não acrescentam nada ao identificador persistente. Uma convenção de designação que foi descrita acima, de nomes, o que o DOA pode fazer? Ele pode fornecer uma persistência semelhante ao DOA sim, então nós temos essa âncora de persistência, ou PANCHOR, então pode permitir a competição.

Nós temos uma convenção de nomes, semelhante ao usado pelo sistema handle, não usamos nenhuma propriedade, podemos usar números, símbolos, até letras, mas nada mnemônico. Então, a estrutura é o mais não hierárquica possível. Primeiro nós chamamos isso de DOA, e DTA de dados, no registro um objeto de estrutura que é algo que contém informações, mas não precisa ser um mapeamento do nome ao endereço de I.P, então o número alocado pelo IANA pelas empresas. Em segundo, são os tipos de dados V ou definidos pelo usuário, os dados vão ficar dentro de um registro ou para fora, onde pode ser encontrado.

Nós temos esse texto, por exemplo, pode ser binário e se há dados, nós podemos colocar os dados aí. Não pode ser muito longo, porque precisa entrar dentro do registro de DNS.

Próximo slide. Isso não é importante. Pensamos em protótipo e um domínio de IoT. Já ouvimos falar na busca de identificadores que não persistentes e ligar a um tipo de dispositivo, então nós pensamos em uma Companhia, chamamos ela de BigCo. Nós assinamos um rótulo, usa dispositivos IoT e usamos um número qualquer. O que pode ser colocado nesse registro para descrever a empresa? Podemos ter uma página na internet que dá algumas informações sobre a empresa, -e-mail de contato ou instalar uma chave pública associada a empresa que descreve o objeto de um modelo de dispositivos.

Pode haver um dispositivo que pode dizer se eu estou rodando a versão correta do software, se não, eu posso fazer o seu download. Com isso, eu passo para o Fernando.

FERNANDO LOPEZ: Eu vou falar em espanhol. Eu sou o Fernando, sou da Universidade Nacional de La Plata. Sou professor e pesquisador nessa Universidade, há aqui uma equipe na Universidade, através do Cabase, começou a trabalhar para criar um aplicativo para registros de DOA.

Seguinte. Em princípio a Cabase registou o domínio persistente ponto lat e uma instituição da Universidade de La Plata configurou os servidores para trabalhar com o nome de domínio. Esses servidores que proveem os serviços de DOA, é uma versão beta de BND e implementam o DNSSEC.

Quais são os dispositivos para os quais desenvolvemos essa demonstração, o MCU controlador de baixo custo, que controla o WiFi, cujo o nome está na tela, e o custo desses dispositivos, incluindo a antena e um pendrive, é de um dólar e meio. Utilizam diferentes linguagens para implementar o demonstrativo, foi modificado a biblioteca LWIP que dá suporte para esses dispositivos, então modificamos o DNS para enviar solicitações de DOA usando os registros do 59 e processas as respostas.

Essa demonstração antes configuravam o registro, nós temos o registro já configurado. Vamos passar para a etapa três, em que o dispositivo será ativado, o que vai solicitar um registro DOA e o setor a receber uma resposta. Dentro da resposta, qual é a versão mais nove de firmware disponível? Um link. Se houve uma versão mais nova, vai haver uma atualização.

Bom, aqui temos o dispositivo e a interface que nós utilizamos, podemos então passar para a tela compartilhada.

Do lado esquerdo da tela, vamos ver o processo de ativação do dispositivo. Está conectado por USB no meu computador para

ativa-la. Vamos ver a captura do trafego de consultas de DNS. Em vermelho vão aparecer as solicitações de DNS e vamos ver os registros já decodificados em azul.

A primeira etapa faz a consulta, nas repostas nós temos a descrição que nós não vamos ignorar aqui o campo de firmware para o URL mais recente, o campo da versão, o e-mail de contato e o campo da assinatura. Isso foi deixado mais lento do que o normal para que os campos sejam mostrados, então o firmware recebeu todas as informações e a etapa seguinte vai descarregar o firmware para atualizado e vai reiniciar com a versão mais nova.

Dependendo da conexão, pode demorar um pouco mais. Nesse momento está fazendo o download da atualização. Bem, enquanto isso, eu quero mostrar a modificação que foi feita, muito pequena. Foi uma semana de pesquisa para entender melhor o DOA, a biblioteca e só três dias para e implementação do lado esquerdo. Vocês veem que o dispositivo foi atualizado, reiniciado e anuncia que tem a nova versão 1.0.

ALAIN DURAND: Eu gostaria de acrescentar uma coisa. Quando tentamos fazer essa demonstração ao vivo, deram alguns problemas com a rede e passamos então para o IPv6. Eu gostaria de agradecer a Universidade de La Plata e a Cabase que realizaram esse trabalho

em só três semanas. Esse é o dispositivo, ele custa um dólar e meio. David Conrad, você tem alguma pergunta?

DAVID CONRAD: Nós temos cinco minutos para pergunta. Na verdade, o Steve tem uma pergunta.

STEVE CROCKER: Eu não quis passar por cima de vocês. A atualização automática chama a minha atenção. Isso é ótimo, exceto se a atualização tiver um problema e você perde o controle do dispositivo. Como você caracteriza a propriedade de segurança?

FERNANDO LOPEZ: Esse dispositivo específico está pronto para a atualização ou só atualiza se a verificação do hash for válido.

STEVE CROCKER: Mas o que acontece se a atualização incita em um bug?

FERNANDO LOPEZ: Então você precisa implementar outra solução, como um receptor físico.

ALAIN DURAND: Eu quero destacar que não é um produto, é só uma comprovação de um conceito, eu gosto de comprovação.

DAVE PISCITELLO: Em primeiro lugar, isso é muito legal. Eu adoro que vocês fizeram algo que é muito difícil de explicar. Conseguiram colocar isso em prática de forma muito clara. Vocês já pensaram nível de objeto para haver um registro dinâmico do dispositivo como parte da interação? Porque quando você faz isso, você está capturando os botnets.

O que poderia ter é um equivalente de um firmware dropper, então tudo que esse dispositivo faria é usar o DNS para entrar e receber instruções, como no comando e control. Então eu sugeriria que, em vez de DOA DTA, chamar só de OBJ – objeto. É muito impressionante.

ALAIN DURAND: Posso responder rapidamente. Sim, estivemos pensando exatamente no que você sugere. Quando nós mostramos isso a empresa, o modelo de objetos, mostramos que havia uma camada mais de delegação para o número de série, então podemos delegar isso para que seja administrado para o objeto e trazer o DNSSEC para validar. Queria lembrar aqui que nesse demo, todas as zonas foram firmadas com DNC sec.

NÃO IDENTIFICADO: O que você descreve é uma modificação do sistema DNS para que funcione com o DOA, mas agora estão utilizando do doi.org/ plano flat space. Questão da persistência ainda não é um problema para o DSN, mas sim questão de políticas na organização, mas o URL continua funcionando e o DOI é tão estável quanto qualquer outro registro produzido pelo sistema DOI. Então, porque vocês decidiram modificar o sistema DNS, visto que vocês estão utilizando as raízes do DNS? Isto é, a implementação do DNS na ICANN.

ALAIN DURAND: Não estamos modificando o DNS, mas criando um novo tipo de RR. Não mudamos servidores, nem os (resolvedores) [00:23:39], nem os bilhões de elementos do DNS que existem. Só criamos um novo tipo de RR.

Para descrever isso, pedimos a equipe de implementação que o fizesse e ao cabo de uma semana, já tínhamos quatro implementações. Quando ao seu comentário sobre que o DOI utiliza um DNS, de fato, ele utiliza um proxy. Enviam todos os dados através de um HTTP, que é enviado a um sistema handle.

Agora estamos tentando evitar isso, evitar que essas questões de privacidade e tudo que tem a ver com tecnologia. Decidimos fazer

algo com a tecnologia DNS simples, que utilizamos durante 40 anos.

DAVID CONRAD: Não sei se há outra pergunta, vamos encerrar a lista de perguntas.

JONNE SOININEN: Eu quero destacar o que o Alain disse, o demo não tem a ver com atualizar os dispositivos, mas tem a ver com utilizar o DNS como funciona, sem ter que modificar nada além da implementação. Obtemos todas as vantagens, inclusive um pequeno dispositivo que é no DNS, isso não causa nenhum problema a capacidade dos dispositivos, mas pode rodar os protocolos tradicionais em um pacote muito pequeno e com pouca implementação.

De fato, não é uma surpresa isso, porque o DNS e tudo que foi feito com os protocolos I.P foram desenvolvidos em uma época em que, provavelmente, o que nós tínhamos a mão teria exigido muito mais espaço. Talvez um desktop, esse é um exemplo excelente e talvez deveríamos considerar opiniões que já temos hoje e pensar nas novas formas de utiliza-lo. Muito obrigado.

RICK LAMB: Sim, é uma maravilha isso, adorei. Eu também sou usuário do ESP8266, vocês modificaram a pilha LWIP para o suporte do DNSSEC? Essas buscas estão validadas?

FERNANDO LOPEZ: Não, agora não verificamos nada com o DNSSEC.

RICK LAMB: Seria interessante isso, porque se utiliza em todos os dispositivos IOT do mercado.

FERNANDO LOPEZ: Seria interessante para esta solução, mas ainda devemos faze-lo.

ALAIN DURAND: Tudo isso começou logo depois da reunião da LACNIC há três semanas. Eu estive falando com o meu amigo do Cabase e decidimos fazer algo. Ao invés de voltar para casa depois da reunião em Montevideo, peguei um navio e fui para Buenos Aires, no dia seguinte me disseram: “você vai para a Universidade de La Plata”. Durante três semanas fizemos um esforço enorme para que isso funcionasse. Etapa dois, vamos fazer o que o David disse, não há que impeça, porque é bem simples.

ASHA HEMRAJANI: É surpreendente, impressionante. Considerando que vocês (inint) [00:27:28] utilizaram dispositivos, outro dispositivo de autenticação para poder verificar o descredenciamento. Quão simples seria incluir a identificação do dispositivo aqui?

ALAIN DURAND: Acho que pode ser aplicado em muitas coisas e na autenticação do (inint) [00:27:53] e também em outras aplicações que precisarem de um identificador persistente, por exemplo, em históricos médicos. Mas isso é algo que utiliza a tecnologia, não para fazer um mapeamento de endereços, mas como forma de trabalhar. Temos um identificador que pode ser muito persistente e essa é uma boa característica para que esse objeto chegue onde quer chegar. Pode ser utilizado em muitos campos diferentes.

JAY DALEY: Estou muito (confuso) [00:28:40] e também horrorizado. Eu achava que essa era uma tecnologia de governança muito bem pensando, do ponto de vista da propriedade intelectual, mas além disso, tem muitos problemas. Acho que deveriam saber o que acontece com a governança, porque há outros elementos que deverão ser modificados e reparados. O que pensa a ICANN sobre fazer isso?

DAVID CONRAD: Uma das atividades que estamos pensando no CTO é uma nova tecnologia, novos identificadores, e o DOA é uma tecnologia que tem gerado interesse em alguns fóruns. Parte do projeto consiste em entender o que é o DOA, como ele funciona, ele é um governo de governança.

Uma coisa que o Alain identificou quando fez suas pesquisas com o DOA, é que aparentemente muito não mudava. A locação de nomes mais incorporado em um modelo de governança diferente, que para a gente não é necessário. O objeto do trabalho é demonstrar que o modelo de governança está separado da tecnologia. A tecnologia pode ser implementada sobre o DNS, então um modelo de governança não é necessário, isso faz parte da demonstração dessa tecnologia. O que nós aqui tentamos entender é como é que a tecnologia fazia isso, como fazia para certificarmos de depender da informação e publica-la a comunidade.

Agora podemos passar a próxima apresentação.

LEONARD TAN: Sou Leonard Tan, vou falar em nome do serviço Ethereum para aqueles que não conhecem as cadeiras de blocos, eu queria mencionar que são as maiores letras distribuídas e tem números

positivos e negativos. Isso foi implementado no passado, através de outros modelos e protocolos, e algoritmos com o Paxos. Isso é utilizado no mundo inteiro, essas cadeiras como o Bitcoin e compensa os custos.

Verificar, através da mineração e também desse incentivo aos ataques. Sabemos como funciona as transações, todas têm uma entrada e uma saída e para que uma atuação seja válida, é necessário fazer uma referência de uma saída anterior.

Como são essas transações? Vamos ver a estrutura. Elas sempre são referenciadas com a anterior até um bloco de mineração, em que o primeiro Bitcoin é produzido, a segunda transação é referente a anterior, e cada uma tem uma produção e uma saída, e está bloqueada com uma chave pública.

Esse sistema, nesse não sabemos se os usuários gastam duas vezes o seu dinheiro, só aparece que sabemos que temos uma série de operações de 2 mil para o Bitcoin, por exemplo, isso é verificado seguindo essas regras. Depois colocamos um hash nesse bloco e isso é compensando, ou os participantes são compensados com Bitcoin. O Ethereum é como os Bitcoins, ou cadeias de blocos, que em vez de armazenar dados e moedas, podem armazenar outras coisas.

O ENS está relacionado com o Ethereum, vou explicar como funciona e depois como é atualmente. O ENS é basicamente uma

forma de fazer o mapeamento que não podem ser lidos por humanos, mas o problema é que pode estar exposto a phishing. Pelo ENS podemos nos referir a registros, contratos e endereços, utilizando nomes. Mas isso não é tudo, também podemos utilizar o ENS oara nos referirmos a outros tipos de registros, como Swarm i inclusive chaves públicas, para buscar de lookup distribuídos com cadeias, eles são transparentes e podem ser atualizados.

A arquitetura interna do ENS é dividida em dois componentes, o registo ENS e os resolvedores. O objetivo principal do registro ENS é manter um mapeamento entre nomes, proprietários e resolvedores. Vocês são proprietários de um nome e podem fazer três coisas, primeiro podem realocar o nome de outra pessoa, mudar o proprietário, mudar o resolvedor, ou criar seus subdomínios.

Aqui vemos a estrutura hierárquica e quanto aos resolvedores, sua responsabilidade é responder a perguntas sobre o nome. Por exemplo: que endereço está associado a esse nome, que registro de endereço IPFS está com esse nome? A resolução de nomes no ENS é muito simples, o usuário faz uma consulta ao registro e pergunta qual é resolvedor para foo.eth, e o (registro) [00:34:59] é o Ox234. Depois, é perguntado ao resolvedor qual é o endereço de foo.eth, e o outros responde Ox234 e etc.

Fizemos um lançamento preliminar do ENS que durou oito semanas. Durante essas oito semanas, lançamos uma série de nomes populares aos usuários através de um processo de leilão. Isso foi feito gradualmente para não aumentar os custos de transações e acabamos no final de julho. Neste processo foram leiloados 150 mil nomes, aproximadamente. Chegamos a um nível de atividade alto, além disso, durante esse processo, foram depositados 168 mil 595 ethers, são 50 milhões de dólares americanos, aproximadamente.

Então se alguém tem um nome, ou ethers, é depositado e fica por um ano bloqueado, depois ele é devolvido a pessoa. A adoção dos clientes do ENS é muito boa, foram adotados diferentes ENS e esperamos que mais clientes continuem utilizando o ENS como tecnologia, à medida que essa tecnologia for amadurecendo.

Também fizemos a primeira oficina ENS em agosto de 2017, com muito assuntos que estão sendo tratados na ICAAN, como resolução de disputas, projetos permanentes, subdomínios, como fazer como seja seguro e como integrar isso com o DSN atual. Então, fizemos uma integração do DNS através do DNSSEC que aqui eu vou usar a cadeira. Começamos com hash de chave DNS, depois a chave foi verificada e assim por diante, até chegarmos a um registro que vemos no último espaço.

Para aqueles que são do DNSSEC, eu passo que é na última parte, ao invés de garantir um registro, temos um texto com o valor do endereço de ethers. Como avançamos com esse processo, o usuário dele ser aprovado. Ele se comunica com a base dados a hora, informa ao registrador que ele é dono do subdomínio, registrando então a pergunta ao Oracle se o usuário já registrou a sua identidade como válida e o registrador, dependendo disso – se for sim ou não – registra o subdomínio no sistema de registro. Nós trabalhamos já com isso e está em fase de teste, isso pode ser feito para qualquer TLD que permita trabalhar com hash, até tipos de TLDs que permitem isso.

Muito obrigado e por favor, continuem conectados para ouvir mais sobre outras novidades do ENS. Não sei há alguma pergunta?

DAVID CONRAD: Temos tempo para perguntas sobre a Ethereum. Eu tenho uma pergunta, tem a ver com o .ETH. O que vocês pensam em fazer no futuro, em relação a domínios de topo, ou com a identificação que utilizamos para os domínios de topo?

LEONARD TAN: .ETH e o código de país para Etiópia não podemos utilizar, mas trocando ideias, estamos pensando agora em fazer uma

integração com sistemas já existente e provar que o ENS funciona, depois vemos o que acontece.

DAVID CONRAD: Eu queria esclarecer se o .ETH, código de três letras, não estão reservados o fato que temos essas três letras e a Etiópia não significa necessariamente que esteja reservado, então se na próxima rodada de gTLDs acontecer, talvez vocês poderiam participar ou não, mas John, sim?

JOHN LEVINE: Muito brigado. Aqui há um problema de segurança que me preocupa muito, porque as cadeias de blocos são tão seguras quanto as minerações. Os bitcoins estão controlados por grandes pools de mineração?

LEONARD TAN: Na China, vocês sabem que faz e sabemos que não são pools e mineração que não estão combinados, ou seja, a maioria dos mineradores estão na China e na maior parte das vezes funcionam por incentivos. Os mineiros vão fazer isso individualmente, dependendo dos incentivos.

JOHN LEVINE: Gostaria de saber se vocês sabem que são esses mineiros, ou vocês assumem que sempre vamos ter suficiente mineiros e também, se há suficientes grupo para que não nos preocupemos e que um grupo só assuma o controle de todas essas cadeias de blocos.

LEONARD TAN: Esse é o nosso objetivo, temos um sistema distribuído para evitar que sejam criados grupos de mineração especializada. Devemos ter um entorno distribuído. Quanto a sua pergunta, sim, podemos trabalhar para que as pessoas não façam grupos ou pools. Eu não sei ainda se podem os fazer alguma coisa, talvez possamos criar um sistema em que todos possam trabalhar em igualdade de condições, mas impedir que eles formem grupos ou pools, isso já é bem diferente.

DAVID CONRAD: Mais alguma pergunta?

PAUL WOUTERS: Eu sou Paul do IETF. Vamos supor que o IETF recebe o domínio IETF neste sistema de nomes, nós pagamos a tarifa por uns anos, todos utilizam o site e se um dia esquecemos de pagar. O domínio cai e fica disponível. Alguém mais registra o domínio? Não sabemos que ele é e nem onde está, então eu início uma causa

judicial, alguém me diz que essa marca é minha e que deve ser devolvida. Com eu recupero esse domínio?

LEONARD TAN: Atualmente a resposta seria que podem recuperar o domínio, mas precisam de um consenso das sete pessoas que fazem parte do grupo de decide, então poderia recuperar a sua marca comercial. Isso é difícil, mas é possível.

DAVID CONRAD: Mais uma pergunta e passamos a próxima apresentação.

JORDI PAILLISSE: Eu gostaria de destacar que quanto a questão da mineração há aproximações que não exigem mineiros especiais para esse processo. A abordagem é diferente, utilizam valor na cadeia de blocos para gerar novos blocos e isso é uma aproximação que poderia ser utilizada. Muito obrigada.

DAVID CONRAD: Muito obrigado. Obrigado Leonard por seu comentário, vamos passar agora a Michael Palage e Pindar Wong que vão fazer a próxima apresentação.

PINDAR WONG: Muito obrigado por nos receber. Hoje nós somos voluntários, eu e Michael, da Sociedade da Internet. Pensando nessa jovem tecnologia, ontem essa cadeia de blocos, não foi halloween, mas foi o nono aniversário da publicação do White paper do Bitcoin. É uma tecnologia muito jovem, os sistemas de nomes, como vocês viram o ENS é uma das chamadas cadeiras de blocos. Há 1 mil 234 já, então algo está acontecendo e todas terão problemas similares.

Se você tem esses endereços de 34 caracteres que são muito aleatórios, seria muito mais fácil de serem gerenciados como usar nomes. Então esse documento que foi publicado recentemente de seis páginas, há algo que está acontecendo que vão necessitar de nomes e de uma governança.

Eu gostaria de agradecer ao Michael por ter me chamado atenção a isso, eu acho que era um risco de longo prazo, mas eu acho que as coisas se aceleraram. A ideia decentralizada, ser o terceiro contato com a ICANN, então tentemos mostrar as oportunidades do horizon e os riscos do novo grupo ao comitê técnico da diretoria.

Ontem falamos mais sobre os sistemas de nomes dessas cadeiras de blocos decentralizados e hoje queremos evoluir um pouco mais sobre esse tema. O problema com a inovação das máquinas é que coisas incríveis acontecem, como o Bitcoin. Os que

perturbam são perturbados também e essa tecnologia de cadeias de blocos vem da periferia. É muito semelhante na internet, isso pode mudar algumas pressuposições.

Ter uma raiz global única, e também mudar a estrutura do mercado. Obviamente, nós temos todo um ecossistema do DNS, mas a minha preocupação agora, usando os exemplos de ontem, é a taxa de inovação desse espaço, assim como o de adaptação de adoção. Nos últimos pontos de contato, usamos exemplos no ENS que funcionam com o DNS atual. Nós temos o BNS - que é o blockstack – que está fora do sistema de DNS. Nós já temos colisões nos sistemas de nomes de cadeiras de blocos, o que ontem eu destaquei foram os identificadores decentralizados.

É preciso entender esses processos. Há inovações que estão ocorrendo dentro dos fóruns tradicionais. Podem haver sistemas como os Bitcoins que estão fora do nosso radar. Eu acho importante que esse documento seja lido e compartilhado. O desafio, como vocês sabem – como na era do telefone – é a pressuposição de que havia antes da internet, que a distância a chamada tinha um preço e mudou muito.

Agora nós temos teleconferências e não nos preocupados com a conta telefônica. Após a internet, nós temos na governança tratados bilaterais com a ICANN, depois temos um modelo multi setorial. Antes do Bitcoin, o tempo era igual a dinheiro, depois

disso, são dados que são dinheiro. Antes da cadeia de blocos, nós achávamos que o centralizado era igual a seguro, se tivéssemos um firewall bom o suficiente, que seria seguro, mas agora está decentralizado.

O processo de desenvolvimento do Ethereum, a reunião está acontecendo hoje e eles tem um processo de desenvolvimento chamados EIPs, que são proposta de melhorias de Ethereum, eles têm propostas de melhorias do Bitcoin. David, na verdade, isso foi modelado em cima do APRICOT.

Ontem nós conversamos sobre fazer um rebooting da rede de confiança e das materiais raízes, aqui o blockstack é um processo diferente e eles tem o seu documento, então a ideia é dar alguns recursos para demonstrar que há outros fóruns que discutem o que está ocorrendo. Há outros grupos dos processos tradicionais padrão e eles estão inovando rapidamente.

Vocês já ouviram falar de Bitcoins e Ethereum, há outro que é o IOTA, que lida com a internet de coisas e há diferentes modelos de governança que podem dar oportunidade a ICANN de considerar esse papel em algumas das questões que identificamos no documento.

MICHAEL PALAGE: Obrigado. Como Pindar disse, o ISOC BSIG é uma iniciativa que estamos tentando implementar para conscientizar sobre essa tecnologia emergente e seu potencial sobre a ICANN. Agora nós temos o Ethereum ENS.

Há uma terceira tecnologia que está no documento e que foi publicado formalmente esse mês, o Blockstack. Essas tecnologias têm potenciais impactos sobre a ICANN. Pode ser evolucionário ou revolucionário. Umas das outras coisas que fizemos no documento foi tentar ver o que os membros das comunidades estão fazendo, especialmente quanto a solicitação de patentes. A VeriSign fez três solicitações de patentes no PTO americano e isso terá impacto. Essas patentes lidam com âncoras de confiança do DNS, objetos fora do DNS e especificamente, fazem referência aos blockchains e os cadastros públicos.

Além disso, outro membro da comunidade da ICANN, Bill Manning, também solicitou uma patente, isso é significativo. Essa é a nossa análise inicial, está conectada as solicitações e ao escritório de patentes americano. Isso dede acontecer em base internacional.

O que a nossa pesquisa também mostrou é que há outros fóruns internacionais envolvidos nisso ativamente. O W3C em conexão com alegações verificáveis, a ISO TC3O7 com relação a

padronização potencial do blockchains e os nossos colegas do ITU, estão muito ativos no SG17 e 20.

O objetivo desse documento não é direcionar a ICANN a fazer qualquer coisa e o Charine sabe disso. A Tricia sempre falou de liderança de pensamentos. Eu acho que a ideia aqui é dar ideias e fazer com que a ICANN saiba que existe essa tecnologia, eu sei que já existe bastante trabalho a fazer, mas eu quero chamar a atenção de que isso existe para que não passe desapercebido e não consigamos lidar com isso.

PINDAR WONG: Nós tivemos a nossa teleconferência mensal ontem e vocês todos receberam esse relatório de seis páginas. Ainda é provisório, uma minuta, mas eu gostaria de dar alguns exemplos sobre as atividades. O que estão no DNS e fora dele. Há uma persistência desses identificadores decentralizados, a questão é que haverá essas marcas de cadeia e como elas se relacionam com as marcas registradas.

Eles têm esses endereços para o Bitcoin e como eu tenho certeza que esse endereço está mapeado pela ICANN. Temos que pensar como isso pode afetar os pontos fortes da ICANN. Já estamos lidando com centenas de blockchains, se houver inflação dos direitos de marca e confusão de marcas registradas, que estão

sendo solicitadas e muito se pode fazer com que atraia membros da comunidade da ICANN a participar em outros fóruns.

MICHAEL PALAGE: Nós só temos dois minutos, eu gostaria de dizer que essa tecnologia está emergindo, são 180 mil nomes registrados no ENS. Se comparado com o número de novos gTLDs em 2012, eu acho que deve ser levando em conta, se nós olharmos o mercado dos nomes de domínios, são 50 milhões e se nós olharmos historicamente, isso equivale a 1998, quando a ICANN publicou o green paper e o White paper. Naquela época havia 1,3 milhões de nomes de domínio a 35 dólares por ano. Eu acho importante buscar paralelos que já aconteceram.

DAVID CONRAD: Há alguma pergunta para o Michael ou Pindar?

WENDY SELTZER: Você mencionou os grupos W3C que usa grupos da comunidade como o laboratório. Há padrões que estão sendo criados desse trabalho, eu sei que o grupo da comunidade do W3C sobre o blockchain está trabalhando com isso, há um vocabulário padrão sobre alegações de atributos. Sim, nós também sabemos que há muito interesse na camada de dados, se houver interesse, eu

gostaria de saber se há interesse em padronizar alguns componentes, eu acho interessante saber.

PINDAR WONG: Eu gostaria só de fazer uma observação. A maior parte – eu sei que é uma grande generalização – mas os algoritmos e os modelos de segurança estão incompletos nesses sistemas. O que é relevante é que tem esses tokens que tem valor econômico, essas fichas, e o valor econômico dessas fichas afeta atualmente a tomada de decisões das pessoas. Pode ser especulativo. Não é tanto em relação a tipologia, mas a um incentivo econômico que leva alguns comportamentos estranhos.

Quando você entrar em uma empresa tradicional que utilizar esses valores digitais, eles querem saber se esses valores lhe pertencem. Em dois anos e meio nós definimos uma área, como é que a gente pode fazer, ou garantir, que os identificadores de identidade legais para a corporação, como é que podemos saber se eles são legais e se então há a oportunidade da ICANN levar em consideração. Em que grau ela pode se envolver nesses outros fóruns e qual é a relação disso com o DNS, como isso pode afetar o DNS.

DAVID CONRAD: Também temos que pensar se isso é uma oportunidade ou uma ameaça. Com isso, passamos a última apresentação do nosso estimado presidente, sobre a gestão da zona raiz inviolável.

CHERINE CHALABY: Desculpe, o que eu estou ouvindo é que a tecnologia do DNS hoje não vai sobreviver? É isso que eles estão dizendo? Ela deve ser melhorada ou substituída por essa nova tecnologia, todos estão de acordo com isso com o nosso CTO?

DAVID CONRAD: Eu sempre achei que nada continua igual, a tecnologia deve se desenvolver ou morrer. Os vetores de mudança não estão claros, há muitas coisas fascinantes no mundo do blockchain, muitos argumentos dizem que pode ser bom, mas eu tenho um pouco de dúvida porque eu não entendo bem essa tecnologia para me sentir confiante o suficiente para dar uma opinião. Essa é uma das razões que eu tenho incentivado a minha equipe para entender essa tecnologia do blockchain e ver como ela vai afetar o ecossistema da ICANN, mais amplo, além do sistema de identificadores do qual a ICANN depende. O que você acha?

PINDAR WONG: A questão de escala é muito séria, eles não conseguem começar a aumentar de escala muito bem. Começamos a fazer a escalada

do Bitcoin, a rede da Visa é de 45 mil transações por segundo. O Bitcoin é de 100 mil ou mais, então eu fico mais preocupado com as comunidades tecnológicas, do que a tecnologia em si.

A comunidade do Bitcoin é impressionante. O que vai acontecer? Eu não sei, mas algo está acontecendo e para que essa tecnologia tenha sucesso, ela precisa ser mais utilizável. Se fala então de designação de nomes, quem sabe, tem que ser mais utilizável. O DNS é o primeiro exemplo, o mais fácil de entender, mas as transações máquina a máquina não precisam do DSN.

Se a pressuposição é um a raiz única, então qual é o sistema? Se nós imaginarmos um mundo diferente, não há certeza estatística. Então quais são as pressuposições e como isso vai afetar as pressuposições da ICANN em 20 anos. Por enquanto, vocês têm as chaves do carro, mas eu acho que a ICANN deveria desenvolver sua tecnologia de blockchain, a sua tecnologia própria.

JAY DALEY: Nós temos que lembrar da pergunta do Cherine, se devem ser separados do DNS, se o blockchain pode mudar o negócio de registros? Muito obrigado.

STEVE CROCKER: Em comparação, o assunto que vou tratar é um problema muito simples, com a tecnologia existente sem adicionar novos paradigmas que possam afetar o ecossistema completo. É uma coisa um pouco antiga se compararmos com todo o material que já foi apresentado, todo esse material avançado.

Não há reconhecimento de voz nesses equipamentos e esse é um trabalho que surgiu a partir de conversas que eu tive durante muitos anos. Tudo isso aqui é verdade, a gente sentou com funcionários importantes de diferentes governos para conversar e falamos sobre essa questão como se fosse uma ameaça séria que, por exemplo, os governos dos Estados Unidos e a ICANN, uma combinação de ambos, ou outros elementos, se poderiam fazer uma mudança disruptiva e imediata.

A solução seria retirar o registro da raiz, o que acontece se desaparece e se aparece a mensagem como não existente? Eles acham que isso poderia acontecer em um período de tensão política muito grave, seria então um movimento ofensivo e ficariam preocupados isso. O que é feito nesses casos é explicar porque isso não vai acontecer, todos esses sistemas de pesos contra freios.

Além disso, se isso acontecesse, o impacto seria relativamente lento e incremental. Teríamos 48 horas para modificar os registros na raiz, então faria uma degradação nos caches de 2% e

isso se propagaria 15 vezes mais rápido que a velocidade da luz, no mundo inteiro. Talvez nem tão rápido, mas vocês me entendem e usam (inint) [01:09:25] do sistema, tentaríamos resolver o problema, buscando outras maneiras de contornar essa situação, e o que aconteceria, o efeito seria bastante diferente do que qualquer funcionário dos Estados Unidos pudesse pensar.

Se algum governo levar os Estados Unidos a se sentir envergonhado, poderiam obriga-los a fazer isso, desta maneira, porque isso afetaria a credibilidade da ICANN e do governo dos Estados Unidos. No entanto, eu sei que as pessoas que entendem isso, entendem bem o que eu estou dizendo aqui, eles têm educação em como podemos pensar nesse problema e ele se transforma em um assunto de discussão para o futuro, no ponto de vista de que é algo para tratar no futuro.

Podemos compensar isso, não através de atividades políticas ou questões organizacionais, mas através de proteção técnica forte, de maneira que seja absolutamente impossível que isso aconteça. Eu vou apresentar a situação e o contexto.

Como eu disse antes, o contexto de pesadelo é que o nome é retirado da raiz de forma abrupta, fazemos na raiz continuamente e é um processo que não é tão fácil. Nunca vamos fazer mudanças na raiz, mas o processo de mudança envolver a

parte afetada, que deveria aceitar ou concordar. Se ele não concordar, a mudança não será feita, mas isso não basta porque haverá traços que esses grupos poderão não concordar e a mudança, mesmo assim, vai ser necessária.

Como eu disse antes, é possível definir e preparar um sistema que impeça esse pesadelo? O conceito básico está baseado em um sistema selado que não pode ser violado, não permite o acesso não autorizado. Temos um sistema atualmente no DNSSEC que isso aconteceu de forma não autorizada, se não tivermos uma chave privada, ela vai ficar anulada automaticamente, o que faz do sistema inoperável.

No entanto, não desativa a chave privada e já não pode ser feita nenhuma mudança, para chegar a um meio termo entre ações inadequadas e não poder fazer nenhuma mudança, o que nós teríamos aqui é tentar alcançar um equilíbrio entre falsos positivos e falsos negativos, ou o tipo um e tipo dois. Neste caso, como em muitas outras situações da vida real, há uma grande diferença no impacto e no tipo erro.

Nessa situação, poderíamos cometer um erro por fazer uma mudança inadequada. Isso é pior do que não fazer nenhuma mudança. Temos (inint) [01:13:01]. Agora sim, podemos (inint) [01:13:05] mas durante muito tempo, havia flexibilidade de quanto tempo demorava para fazer uma mudança. Esse tipo de

equilíbrio funciona muito bem, esse conceito básico do sistema selado, que não pode ser acessado sem autorização, temos um sistema atualizado com um controle split, temos uma base de dados que não podem ser acessados sem autorização, temos um sistema atualizado com um controle Split, temos uma base de dados PTI pela IANA e tudo isso deve estar sincronizado a manutenção da VeriSign e comunicações e poderíamos colocar tudo isso em único lugar. Não podemos fazer isso se não estiverem em ambos.

Podemos pensar também nas raízes divididas em pequenas porções, com uma porção para cada domínio de topo e um pouco de informação para cada domínio de topo. Todas essas informações associadas com todos os domínios é o que constitui o conjunto de servidores associados, depois temos o DNSSEC, temos as chaves, temos o DS registrado também a outros detalhes, é uma discussão bem complexa. Também importante saber como nós lidamos com os registros de servidores raiz e com os registros autorizados. Essas questões podem ser resolvidas facilmente. Eu mencionei também os registros Glue, e esses são detalhes que eu não vou tratar nessa sessão.

O conceito que eu também destaquei é que não é necessário fazer nenhuma mudança na porção de TLDs na raiz em relação a aprovação dos operadores. O TLDs, portanto, as vezes é um operador e se ele decide fazer alguma alteração e não gosta, ou

nada acontece de imediato, aqui teremos um problema diferente. Também podemos mencionar que é importante tem um sistema robusto, mas há outros aspectos que devemos levar em conta.

É importante pensar isso, sem falar em um token no hardware, isso poderia ser feito com software, mas imagine que temos um token no hardware. Um dispositivo que é utilizado por uma TLD e que é utilizado como dispositivo para identificar e autorizar uma mudança potencial, se não fizer isso, essa mudança não poderá ser feita. Agora, como é que isso é recebido, em primeiro lugar, e como é feita a associação entre o operador e o dispositivo? Esse é um processo diferente que exige separar essa ideia de que não é possível fazer nenhuma alteração sem uma aprovação previa. Precisamos de um processo mais complexo, temos a cerimonia da mudança de chaves. Em outros processos, pessoas que entram em contato e que trabalham juntas são pessoas suficientemente independentes, para evitar colisões e outro tipo de impressões, ou para que o processo seja lento, deliberado, visível e documentado.

Essa é uma das mensagens que demonstra bem como esses processos são lentos, se nós pensarmos em uma realocação. Outro caso, por exemplo, uma chave se perde ou ela se queima, são situações que poderíamos imaginar, então deveríamos passar por um processo lento, muito visível e documentado. Esse

é um controle político de mutuas partes. Nem todos juntos poderão fazer isso, mas temos essa situação. Vamos imaginar que temos 1500 operadores de TLD de raiz atualmente e existem 1490 vão demorar mais. Os últimos mil, vão demorar de dois a dez anos, então esse é um dos processos de transição.

Todos os projetos devem estar preparados para operar com o sistema atual e com o novo sistema, isso seria muito bom. Poderíamos pensar em modificar o sistema, utilizar depois os nossos dispositivos para cada operador de TLD e já estar pronto para ser utilizado, serão enviados e depois aqui, vemos o processo de atualização da zona raiz, vemos mudanças que entram na caixa de operador do TLD à esquerda, isso para a função da IANA que valida solicitação, aceita e envia a VeriSign e desse diagrama faz duas coisas, a base dado gera a zona raiz e deixa fora a geração de raiz e de assinatura, adiciona uma compilação do diagrama, mas isso para depois deixar um grau de simplicidade. É um processo de distribuição de duas vezes ao dia, como manda uma distribuição da zona que é feita disponível para operação dessa raiz em 13 letras, e depois do processo de atualização feito hoje.

Na coluna do meio temos um sistema hermético e selado, com dois grupos diferentes que estão operando e que são dois sistemas de hardware fisicamente, ambos são invioláveis, tem um protocolo robusto e os conectam entre si. Aqui vou repetir, há

duas classes de transições, as comuns, com mudanças comuns e os registros de DS e chaves do DNS. Também, por outra parte, temos a transação que passa pela via rápida, até que operador diz que quer essa alteração, então tem uma autorização para fazer a mudança, pode ser aprovado ou não. Mas isso não pode ser feito sem a autorização do operador. As mudanças mais importantes são de controle que exigem que seja seguido esse processo mais elaborado.

Esse é outro diagrama de uma operação comum, e depois o que nós temos, imagine que aqui em cima nós temos uma mesa de conferencias, temos muito pessoas junto a mesa e elas estão desenvolvendo processos. Isso é muito parecido, por exemplo, como nós fazemos a cerimonia da chave com computadores confiáveis a comunidade, basicamente aqui repetimos o que eu já disse hoje. O suporte de órgãos de supervisão, seria um grupo de pessoas confiáveis e se nós quisermos explorar isso, podemos nos próximos passos, apresentar um projeto conceitual e documentar, compartilhado, e talvez podemos dividir em três dias de trabalho paralelos, com vias paralelas, explicando qual é o processo e criar protótipos de operação entre o operador de TLD e o sistema. Poderíamos criar um protótipo de como o sistema funcionaria.

Esses três passos poderiam ser feitos em qualquer ordem, isso para poder colher mais informação. Acho que é o último slide,

aqui tem sub conceito e faz tempo que eu estou pensando nisso, eu nem me lembro quando eu comecei a trabalhar nisso, mas eu deixei isso de lado quando o processo de transição começou. Eu pensei: que bom. Isso iria distrair e causar confusão, mas a transição acabou e estamos aqui nessa instancia. Muito obrigado.

DAVID CONRAD: Antes de passar as perguntas. Eu queria destacar que a minha equipe está pensando e planejando emitir um RFP com dois tipos de mudanças. Um é de mecanismos digitais da zona raiz, e tem a ver com a evolução, essa é uma abordagem revolucionária que reestrutura a maneira que nós fazemos as coisas, uma das ideias era incorporar essa ideia de termos uma ideia inviolável e uma abordagem revolucionária. Isso fazendo uma convocação para apresentar proposta, um RFP. Alguma pergunta? Bom, espero que não haja muitas perguntas, não seria bom porque não poderíamos ir ao cocktail.

ROD RASMUSSEN: Sim, essa abordagem é bem interessante. Eu me pergunto se a administração da zona raiz, eu acho que os TLDs estariam interessados com os modelos de combinações diferentes, porque aqui entramos na raiz?

STEVE CROCKER: Sim. Essa mesma tecnologia pode ser aplicada em todos os níveis e é só isso.

DAVE PISCITELLO: O único modelo de ameaça é que leva as pessoas a se preocuparem, pensando que isso não funciona e realmente eu gostaria de ver um modelo de ameaça, uma análise de custo e benefício, para entender bem qual é o resultado final, onde altera isso. As ameaças que já temos para ver como nós mitigamos, porque eu não vejo que as ameaças sejam algo tão obvio que não se deve pensar que os Estados Unidos vão se vingar.

STEVE CROCKER: Eu tentei abordar isso bem no começo, mas para aqueles que estão sentados no centro do mundo, como você e como eu, pensamos que isso é ridículo e ninguém deveria preocupar-se com esse tipo de mudanças, mas se nós pensarmos em locais mais afastados, então poderemos sim pensar na questão de estarmos em risco, um risco para economia do país e que chega ao fim. Então, esse é um modelo de ameaça. Última pergunta.

LARS-JOHAN LIMAN: Essa é uma forma de evitar a delegações de serviços?

STEVE CROCKER: Eu tentei mencionar isso antes, eu tive uma conversa interessante há alguns anos sobre essa questão com um operador mito importante de TLD e eu perguntei a ele quanto tempo ele deveria considerar para fazer mudanças nas suas operações com o servidor com o novo nome. Ele disse que em 48 horas máximas, isso aconteceu com o with.COM que essa mudança pode ser feita em poucos segundos, um minuto talvez.

Então eu perguntei: com quanto tempo vocês planejam isso? De seis dias a oito semanas, é bem isso, porque naquela época o que ele queria dizer é que havia uma solicitação, mas eles não sabiam se era expedida e se poderia permanecer, no entanto, hoje a situação é diferente, é bem melhor, e eu acho que os operadores de TLD vão ter que fazer mudanças na configuração de servidores de nomes, e que eles não se encontram e uma situação que possam fazer isso instantaneamente.

Por exemplo, recebemos uma solicitação e isso não é feito, temos o processo de encaminhamento e temos processos formais. Para isso, seria um início de um processo em que isso não acontece, mas que passa por um processo mais extenso e se transforma em uma demora, em vez de uma denegação absoluta.

LARS-JOHAN LIMAN: Eu estou pensando nisso por uma questão política, principalmente deveremos resolver isso, do ponto de vista político.

DAVID CONRAD: Então vamos chegar aos assuntos gerais e quanto aos assuntos gerais, é que todos os interessantes podem ir para o cocktail, devem ir até o saguão do hotel, a porta principal, com o ônibus que nos levarão onde está o cocktail, é um deck observação e parece muito bonito. Temos fotos nas melhores revistas de viagem. Muito obrigado a todos e a gente se encontra de novo em Porto Rico.

[FIM DA TRANSCRIÇÃO]