PRAGA – ASO/NRO – apresentação em RPKI
27, junho, 2012 – 12:00 to 12:30
ICANN - Praga, República Checa

PRESIDENTE DRYDEN: Bem-vindos à ASO NRO. Houve muito interesse por parte do GAC para que saibamos sobre esse tema. A comunidade esteve trabalhando nisso. É por isso que vou passar a palavra para o senhor John Curran que se vai apresentar e apresentar os seus colegas.

JOHN CURRAN: Sou John Curran, presidente da NRO, Organização de Recurso de Números que é uma organização de apoio à ICANN para os endereços.

Tenho aqui na mesa o presidente da organização e assessoria de suporte de nome, que se chama Louie Lee. Temos os CEOs das RIRs que constituem várias dessas organizações, me incluindo a mim pela ARIN, Raul Echeberria pela LACNIC, Paul Wilson pela APNIC, e Adiel Akplogan para AfriNIC.

Também vamos abordar algumas questões sobre o que é a RPKI.

GEOFF HUSTON: Obrigado a todos. Esta é uma apresentação muita técnica já que abrange tecnologias que não estamos acostumados a ver usualmente. Se encarrega de tecnologias que se relacionam com a segurança da nossa infra-estrutura e das nossas comunicações. É interessante que existem várias maneiras de ser ruins na internet, há muitas maneiras de fazer coisas ruins. Certamente a gente pode enviar muito SPAM e pode

tentar corromper a operação do sistema de DNS e o DNS está sob constantes ataques. A gente pode também tentar enviar pacotes muito particulares a certas máquinas para que elas façam coisas que nunca teriam a intenção de fazer.

O mesmo acontece com os vírus. Porque os vírus mudam a operação do sistema que infectam, mas há outros ataques que são até mais incômodos. Esses ataques não tentam modificar a operação da sua máquina, mas na medida em que a máquina está funcione corretamente o ataque vai ser mais bem sucedido. Esses dois tipos de ataque não só acontecem a máquinas individuais, mas também na infra-estrutura da internet em sim mesma.

O primeiro se dá no nome de domínio que é um tema sobre o qual estamos muito familiarizados faz muitos, muitos anos e os esforços para apresentar soluções sobre a segurança do DNS, o DNS e a sua implementação como vemos nesta reunião da ICANN já estão em andamento. Muitos workshops já estão em atividade e é muita compreensão.

O roteamento é diferente. É um problema muito, muito difícil. Para poder compreender como redirecionar esses pacotes para o destino quem tem a intenção de chegar é necessário utilizar alguns algorritmos sofisticados que foram estabelecidos o roteamento. É um problema muito difícil, mesmo em termos da sua tecnologia subjacente. Quando nós construímos por primeira vez o sistema de roteamento e estou recuando 40 anos, na década de 60, foi feito dentro de um ambiente de pesquisa e esse ambiente tende a ser, ou a pensar, coisas bem básicas.

Uma dessas questões é que existia certos jogadores, todo mundo tem essas mesmas suposições e os algorritmos se baseiam na confiança mútua que é muito importante para a internet. A confiança mútua não é o ambiente no qual vivemos. Mas como contra-arrestar ou equilibrar essa confiança mútua.

Se nós pensamos que são todos bons jogadores qual é a resposta? A resposta é que todos tem que checar tudo, verificar tudo, mas essa função de verificação é extremamente difícil. Porque cada um dos jogadores que faz o roteamento tem que reunir muita informação todo o tempo, sobre endereços e políticas de roteamento. Não há um repositório centralizado dessa informação, nem técnicas bem entendidas ao longo de tudo isto. É um trabalho muito difícil. Então em lugar de fazer isso vamos aplicar uma solução que é eficiente quanto ao custo. Essa eficiência no custo significa que no limite há uma coisa um tanto vaga.

As coisas que acontecem ao sistema é incerto. Houve alguns incidentes bem notáveis no passado. Talvez muitos estão na área de segurança, e são conscientes de incidentes faz um par de anos, um par de horas em que um ISP n área da Ásia conseguiu bloquear internet em grande parte do planeta, no Youtube. Isto é politicamente da viagem de certos vírus. Eles se propagam na internet. Mas as questões de hoje são vulnerabilidades do amanhã. É possível que algumas coisas se façam por acidente e outras por intenção. Temos que ver que o sistema que estamos trabalhando não é bom. Vão ver que os seus próprios podem ser seguros, seu laptop pode ter a melhor atualização, e a web pode estar bem, funcionando tudo bem, mas se o sistema de roteamento está em compromisso, os pacotes não vão para o destino que tem que

chegar e podem passar por certos pontos não intencionados e navegar por um lugar ao qual não tem tem que ir.

Obviamente podemos ver cada um desses pacotes. Os pacotes são de mais. Não podemos levar em consideração tudo. Não podemos equipar os roteadores com pessoas por trás deles porque são muitos. Tem que ser um sistema automatizado que opere na mesma velocidade que os pacotes que correm por eles. O que temos que fazer é colocar um discriminador na nossa infra-estrutura que permita detectar e excluir as tentativas de colocar informação falsa no sistema de roteamento. Temos que poder distinguir o bom do ruim, automaticamente.

Há poucas ferramentas básicas que consigam isso no sistema público, como cada um na criptografia vai dizer que é fácil criar criptográficas, encriptação de uma só vez, mas não é tão assim, fácil criar sistemas criptográficos quando as duas partes vão trocar informação e se encontrar antes para trocar segredos. Nós não temos esse sistema. Temos um sistema em que as partes que estão tentando trocar essa informação nunca se reuniram e não vão se encontrar jamais, nem podem se encontrar. Isso limita possibilidade das ferramentas que temas a um conjunto bem pequeno. E esse é o conjunto da criptografia pública e privada. O que estamos utilizando em realidade são assinaturas digitais convencionais que é assinado uma senha privada e só ela que pode destravar algum artefacto digital.

O seguinte como enviar para essas redes públicas ao longo da rede, como injetamos essa autoridade confiável, dentro da rede. Então temos que entender em primeiro lugar como descrevemos a confiança. Eu tenho o endereço e o meu endereço IP é um número, o que é um

número um pouco estranho, 3 10 1.000.000 220. Como sabe o resto do mundo que esse número, esse endereço IP é válido, genuíno. Porque a internet tem que trabalhar de maneira única. Temos um sistema que atribui de maneira singular as eleições individuais para o sistema. É o marco de atribuição de endereços e essa hierarquia atribuiu autoridade em IANA, depois envia para os registros nacionais e talvez outros registros locais, para diferentes máquinas.

Meu número então é único porque a APNIC me deu e o número de APNIC é único porque a IANA deu a APNIC. Se pudéssemos descrever essa cadeia nos daria aos crachás para criar confiança no sistema de endereços. É por isso que o que tentamos fazer é não incorporar novos dados, mas reformatar o registro para permitir que os mecanismos de autenticação sejam construídos por cima dela. Isso nos leva depois ao conceito de um certificado de recurso.

Um certificado é um artefacto bastante velho no nosso mundo. Há certificados digitais, o X.509 que se refere há vários anos e estamos falando de um padrão bem comum. É um instrumento digital que reúne recursos de números e uma senha pública que assina as senhas privadas. Esse alguém que possa dizer esse endereço é meu, vão ver se eu estou online ou não, vão ver se eu estou mentindo, vão poder autenticar a minha afirmação. Acho que isso é bastante poderoso e simplesmente diria que não é um coisa que a RIR inventou por si próprio. Estivemos trabalhando neste espaço em conjunto com RIRs e dentro da força de trabalho desde 2006 para gerar uma tecnologia viável e padrões que permitam construir e trabalhar e operar de uma maneira confiável.

Esta é uma maneira de publicar os dados, os mesmos dados que sempre publicamos em formato diferente porque agora esses certificados X.509 são esse tipo de certificado. Quem tiver, pode optar por gerar um certificado digital que diz que o seu par de senhas está associado singularmente com os endereços de IPs, e se deriva diretamente do banco de dados de registração subjacente. Portanto essa base de dados mostra a mesma informação.

Então agora temos esse conceito e é como a hierarquia do nome de domínios. Trata-se de uma hierarquia de certificados digitais que é conhecida dentro do mundo de segurança, porque eles adoram criar termos novos. Sempre usam termos novos quando um velho poderia funcionar corretamente. Então, dentro dessa hierarquia eles gostam de infra-estrutura de senha pública. É PKI. É uma hierarquia de certificados que fala não apenas da minha identidade, não do meu papel, não da questão que convencionalmente fala um certificado digital, mas é uma hierarquia que fala dos recursos numéricos de IP e isso permite declarações, como que eu sou titular de um endereço em particular e que esse endereço pode ser assinado digitalmente por outra pessoa qualquer e, qualquer outro pode verificar se essa afirmação é verdadeira ou não.

Quando me refiro a qualquer pessoa estou dizendo qualquer pessoa ou coisa, inclusive qualquer roteador, qualquer elemento de switching dentro da rede e até qualquer interface de comando para suporte operacional da rede. Se podem dizer coisas que se relacionam diretamente com como os endereços da internet são geradas e roteadas. O Geoff, o proprietário de 1.1.0/24 posso autorizar AS23456 e somente essa rede vai se rotear para mim. Se qualquer pessoa tenta

atacar o meu endereço eu vou saber que está mentindo, mas qualquer outra pessoa na internet também vai saber que ele está mentindo. É muito mais difícil mentir quando a gente sabe que está mentindo.

Esse seria um novo desenvolvimento para nós. A segurança é muito difícil para nós e a comunidade teve longos debates a medida que vamos avançando. Somos conscientes que em vários regimes houve alguns certificados digitais e interesses também legislativos em que o regime digital revogue, sejam revogados por medidas judiciais com os tribunais.

A comunidade tem discussões a respeito do tema de ser obrigados por um tribunal a revogar, ou alterar um certificado. Não temos qualquer resposta para isso, mas observamos o mesmo processo judicial que poderia existir ou encaminhar um proprietário de um registro muito facilmente a mudar o conteúdo do registro, revogar um certificado, mudar o conteúdo do registro, é a mesma coisa.

Por isso dizemos que não é uma solução mas também não não apresentamos o reduzido os fatores em torno desse aspectos das pressões externas sobre a integridade da todalidade do sistema dos registros. É uma hierarquia como o DNS e se a pessoa consegue comprometer a raiz, o efeito vai, anda para outras partes do sistema e se compromete muito alto nessa hierarquia e os danos e os riscos potenciais são muito grandes. Mas, isso é semelhante a comprometer os certificados que utiliza Visa ou MasterCard.

Se vocês pensam no caso que podem acontecer, olha se se comprometem ainda. Muitos dos sistemas digitais da atualidade, que tem a ver com grande parte da nossa economia, tem os mesmos

problemas. A indústria gerou muitos padrões para assegurar a integridade das operações do certificado. Padrões FIPS que tentam gerar as senhas para conseguir essa segurança, utilizamos essas senhas e não podemos fazer de outra forma.

Mas, com certeza que tentamos, estamos tentando fazer o melhor possível. Esse sistema de gestão de senhas, os certificados estão no limite dos padrões da indústria nesse sentido. Também há uma questão referida a estabilidade. Há muitos sistemas a prova de falhas, mas o sistema atual particularmente na área de publicação de políticas, confia na existência de um lugar único no qual essas políticas estão alojadas, hospedadas e é a forma que se realiza da integridade dos dados, assinados são diferentes. Se eles são assinados todos podem ser publicados. Qualquer pessoa que receba qualquer cópia, pode dizer imediatamente se é confiável, se é uma cópia confiável do original. Porque digitalmente não pode ser distinguido. Cada um dos senhores pode pegar uma cópia e replicá-la e qualquer que pegue esse artefacto republicado pode ter certeza de que é exatamente igual ao original, bit a bit.

Então aí sim há questões de fracassos, de insucessos, mas por outra parte essa informação assinada achamos que é muito mais flexível dentro da infra-estrutura.

Por favor, a próxima, o próximo slide.

Então, onde estamos agora. Estamos muito avançados nesse processo porque o sistema de roteamento tem vulnerabilidades e o sistema de nome de domínio de internet é muito importante. Nós estamos tentando ganhar velocidade quanto a infra-estrutura de certificados,

muitos certificados regionais, tentando incorporar nos próprios sistemas. Os membros dentro dessas comunidades em particular, podem gerar os certificados segundo desejados.

A partir de agora os RIRs continuam trabalhando na comunidade para completar a informação. Há muito trabalho especializado e há alguma diferença enquanto a implementação. Portanto alguns RIRs estão fazendo as coisas sutilmente diferentes, mas o resultados serão vistos num futuro próximo. Mas estamos já dentro dessa área e queremos que esses registros regionais acabassem esse processo em forma rápida.

O certificado não é tudo. Temos que incorporar esses certificados aos sistemas operacionais atuais e temos que ter também apps como outro sistema. Estamos trabalhando não só com RIR , mas também com IETF e com outros organismos públicos para gerar módulos de plugin. E também temos que distribuir e sincronizar essa informação a respeito da validade de qualquer endereço e rota na internet em todos os momentos. Para quê? Para assegurar que esses dados estejam completes e exatos o tempo todo, ao mesmo tempo, ou por outra parte o IETF está trabalhando para assegurar o protocolo de roteamento específico o PGP. Estamos avançando também, resolvemos algumas questões referidas a integridade e a integridade das sessões e da integridade também da origem, mas agora estamos vendo que temos um problema de cadeia que nos leva a ter uma pausa para pensar. Mas, todos somos muito otimistas de pensar que entre todas as curvas o uso mais efetivo do encriptamento, e o conhecimento em uma prática mais comum da criptografia, na nossa comunidade, e com isso vamos resolver esses assuntos como já se foram resolvidos outros, então isso pensamos que vamos conseguir num futuro próximo.

Vamos passar ao próximo slide.

Eu acho que já apresentei tudo o que queria falar e com prazer vou responder qualquer pergunta. Muito obrigado.

NOVA ZELÂNDIA: É uma apresentação muito importante. Eu acho que a pergunta óbvia para o GAC é tem uma política pública ou algum impedimento em termos de política pública para conseguir isso? Uma coisa que o GAC possa fazer para acelerar a implementação desses protocolos? Essa é a pergunta. Muito obrigado.

GEOFF HUSTON: Com certeza alguns organismos internacionais não tem muita consciência da natureza desses problemas e foram muito ativos apoiando investigação e desenvolvimento de alguns organismos por exemplo dos Estados Unidos que eu trabahei durante muito tempo. Mas, não são as únicas instituições e únicos países. Já vimos muitos outros que são conscientes e que apoiam atividades neste sentido, então isso é muito bom.

Temos essa questão, este assunto de que não operamos sobre os termos e condições de imunidade de um âmbito legislativa judicial, então quando vemos os certificados nas comunidades elas expressam a preocupação de que um tribunal diga que deve ser revogado um certificad, proque as consequências dessa revogação não é a pena de que não vão ter esse endereço. Mas também os certificados dos endereços de roteamento também desaparecem e isso significa que tira a validade da presença desse endereço e que isso desaparece para

todos os demais também. Quando introduzimos a segurança também introduzimos outros fatores que são novedosos em alguns casos. Não tenho certeza de ter todas as respostas. Não sei se estou procurando resposta neste momento. Mas entre as coisas que podemos falar na política pública essa é uma das questões.

PRESIDENTE DRYDEN: Muito obrigado. John eu queria responder também e vejo que Paul pediu a palavra.

JOHN CURRAN: A respeito de incentivar essa política, acho importante lembrar que a decisão do fornecedor do serviço de utilizar a RPKI e de ter a segurança na informação do roteamento na política, de roteamento é uma coisa voluntária. Os fornecedores de serviço decidem se vão participar nessa infra-estrutura, na RPKI, porque quando fazem a informação de roteamento, se estiver menos comprometida por outra, da mesma forma decidem prestar atenção a nossa informação da RPKI, porque quando recebem informação do roteamento, vão ter menos possibilidade de receber informação incorreta, suspeita de roteamento. Então muitos utilizam a nossa RPKI e prestam atenção aos dados recebidos. Mas, para os fornecedores tudo isso se baseia numa decisão voluntária. Nossa região está o Canadá, Estados Unidos e 26 economias do Caribe.

Eu sou consciente que nos Estados Unidos há grupos de confiabilidade de internet, há um grupo de melhores práticas patrocinados pela FCC, que faz referências a melhores práticas na segurança, e no roteamento.

Então há forma de ver tudo isso. Mas isso não é um coisa que os RIRs seja feito. Somos a localização natural para fornecer a infra-estrutra. Tanto a publicação, quanto a observação dos dados recebidos tem a ver com a decisão voluntária dos ISPs.

PRESIDENTE DRYDEN: Obrigado. Paul?

PAUL WILSON: John cobriu muito bem outros temas que talvez devemos lembrar para ver o sistema atual como onde os RIRs oferecem os detalhes do registro dos nossos endereços que nós atribuímos os certificados de alguma maneira.

A medida em que tem uma assinatura com o mesmo registro, se maneja da mesma forma que um email com uma assinatura digital que diz qual é a origem de quem assina. Ou seja John se referiu a esse processo que é importante, considerando que o fornecedor decide fazer através de uma opt-in da opção de participar. Ou seja, de ver o que acontece numa metade da equação e por outra parte de ver o que acontece com aqueles dados que recebe. Esse é um sistema que evolui de forma totalmente compatível com o processo consensuado do nosso sistema de RIR, que é ascendente e não imposto obrigatório dos níveis mais altos para as bases.

Pelo fato de que estamos fazendo a apresentação que nós sentimos que o nosso sistema esteve sendo desenvolvido através dos tempos com esse processo, e que os RIRs também tiveram seu processo durante anos e que as perguntas com o sistema ampliaram-se agora, nos últimos

tempos e pensamos que era útil que o GAC tivesse essa perspectiva, essa atualização, com respeito a como funciona o sistema. É também para nos assegurar de que haja um entendimento comum, com referência a essa opção participar ou esse sistema de opt-in, que já descrevemos, a diferença do que se fazia no passado.

PRESIDENTE DRYDEN: Tenho agora Portugal, Noruega, Malásia e a Comissão Européia.

PORTUGAL: Muito obrigado pela clareza nessa apresentação. É uma questão muito téc nica e foi apresentada numa forma que todos entendemos. Sabia do sistema através dos esforços de RIPE. Agora a minha pergunta tem a ver com uma coisa que já foi mencionada pela Nova Zelândia. Levando em consideração o papel do GAC seria interessante saber o que é que pensam os senhores que são coisas que nós poderíamos fazer do ponto de visto do assessoramente que damos a comissão, ou qualquer outra coisa que pareçam que possamos fazer para ser claro, não sei de que forma podemos participar, do ponto de vista de aprovação de políticas a nível nacional. Ou simplesmente para gerar consciência. Seria bom se pudessem deixar claro o que os governos podem contribuir neste sentido.

PRESIDENTE DRYDEN: Muito obrigada, Portugal. Raul, você pode responder?

RAUL ECHEBBERIA: Obrigado Sra. Presidente. O objetivo pelo qual estamos aqui falando com o GAC aqui é porque queremos comentar o que estamos fazendo, para que os governos saibam disso. Acho que é uma mudança importante para a internet, um projeto que como falou Geoff leva já muito tempo de trabalho e se fez um investimento muito grande em termos de tempo, trabalho e dinheiro. É uma coisa grande para a internet e é importante que os governos conheçam.

Provavelmente acho que essa é a principal maneira que nos podem ajudar, se é o que querem fazer, ou seja, gerar consciência. É isso que podem fazer gerando consciência nas indústrias locais, como diz John temos um caso ilustrativo nos Estados Unidos e isso também pode ser feito em outros países, outros lugares.

PRESIDENTE DRYDEN: Muito obrigada, Raul. Tenho a Noruega, Malásia, Comissão Européia, Uruguai e o Reino Unido.

NORUEGA: Muito obrigado Sra. Presidente. Muito obrigado Geoff pela atualização, pelo refresco. Obrigado por toda essa informação tão valiosa que nos deu. Acho que é importante para nós como governo saber o que acontece com esse sistema, porque se tomam medidas de segurança muito importantes na internet. Também queria comentar algumas das perguntas, das questões que tem a ver com as políticas públicas. Acho que esse tema que tratamos aqui nos leva a pensar que podemos criar consciência e também propiciar as melhores práticas nas regiões com regulamentação de diferentes partes da Europa, da qual pertence a

Noruega. Temos faculdade como entidade regulamentadora para estabelecer medidas de segurança para os fornecedores de serviços de internet, caso consideremos que isso é adequado fazer. Ou seja, alí, poderíamos trabalhar na Noruega desta forma. Podemos também estabelecer esse mandato para os ISPs noruegueses. Mas isso também pode se transformar numa melhor prática entre os ISPs do mundo e com a internet não pode ser aplicado medidas de forma isoladas, porque isso é um sistema mundial. Ou seja, é importante ver deste ponto de vista.

Uma pergunta de natureza técnica. Na verdade são duas, uma mais técnica e uma que tem a ver com prazos.

Quando o sistema estará operativo? Quando as aplicações do roteamento, tudo estará pronto e quando será feita a pradonização para ter tudo isso já implementado e finalizado?

Outra pergunta tem a ver com os certificados dos RIRs. Vão ter certificados assinados que serão, que poderão ser utilizados para assinar os recursos. Porque há algumas inquietações por parte do governo, não por parte do nosso, mas sim de alguns outros, no ssentido de que se os RIRs vão ter certificados assinados e vão ser controlados por outra parte que isso talvez possa, caso revogado esse certificado, possa estragar todo o roteamento na internet. Então, estou interessado em saber como vai ser construída essa cadeia de confiança, dentro do sistema da PKI.

PRESIDENTE DRYDEN: Obrigado Noruega. Alguém quer responder. Geoff?

GEOFF HUSTON: Quando se fala de melhores práticas em contraposição com requisitos regulatórios, para implementação e uso desse tipo de terminologia é verdade que DNSSEC se eu tenho Geoff.net ,que eu assine ou não é irrelevante salvo se .potaroo.net esteja assinado também. Porque isso é importante em DNSSEC chegar a esse nível da raiz. Mas no nosso sistema de roteamento, nós não temos a facilidade de estabelecer a hierarquia de roteamento. Se nós temos, estamos seguros com O BGP e depois passamos essa informação numa sessão de internet que não implemente essa forma de BGP, toda informação de segurança se perde. Quando chegamos a outro lugar que sim, aplica, utiliza, aí não vai chegar a informação.

Então BGP é um protocolo que vai dar uma grande quantidade de benefícios. É um desses sistemas que se todos utilizássemos daria um benefício a nível universal. Se quem faz é as ilhas, ou se faz em parte, temos que ver quem pode se beneficiar e a quem pode afetar do ponto de vista do roteamento, porque esse benefício se vê reduzido de forma ampla, grande. Então temos que pensar cuidadosamente nesse tema, do que é uma melhor prática de segurança, de infra-estrutura, a nível nacional e regional. E temos que pensar também com cuidado, como ampliar ao máximo tudo isso e por outra parte, não impor custos proibitivos , de alto risco, ao entorno operacional. Então não estou tendo uma resposta clara. Tudo isso faz parte de uma agenda, do processo de política pública a nível nacional que tem que tentar de fazer implementação por parte, de forma isolada da tecnologia, porque isso não é tão benéfico como uma implementação universal.

PRESIDENTE DRYDEN: John, eu sugeriria que talvez poderíamos falar um pouquinho de BGPs e entrar em contextos porque nem todo mundo conhece essas normas.

JOHN CURRAN: Eu sou John Curran e eu vou assumir as outras três perguntas implícitas que estão dentro da pergunta explícita.

Em primeiro lugar eu quero dizer que com respeito aos tempos, cada um dos RIRs, tem os seus próprios cronogramas de implementação e isso para estrutura, para os certificados digitais, seja para emissão, para veiculação dos fornecedores de serviço. Temos também outros mais avançados.

A maneira que funciona a responsabilidade em nossa região é tal que temos que tomar muitas providências, para tentar associar nossas atividades de assinatura digital, de maneira que não haja repúdio, que possamos confirmar que o ISP realmente solicitou os certificados. Isso requer demais trabalho da nossa parte, talvez nós sejamos os mais demorados e estamos pensando entre agora e o fim do próximo ano para ter isto em produção. A maior parte dos outros registros nacionais, já tem os registros prontos. Hoje é um tempo muito menor.

Com relação aos certificados que usam os RIRs e a ancoragem do que chamamos a confiança, ou a âncora de confiança, há muita informação para estabelecer um elemento digital no sistema que dê confiança. Se falarmos em vários roteadores que são ISPs podem configurar cada um dos 5 RIRs com essa âncora e desse jeito, vocês ali pensam que as coisas foram emitidas nesses 5 RIRs e também tudo que está junto com isso.

Então seria conveniente ter uma única âncora de confiança global e que a IETF poderia emitir isto junto com RIR. Nós vamos nos reunir com a equipe de Elise Gerich, para mostrar que isso pode ser factível. Então neste caso teremos a possiblidade de usar o nosso PKI, não com 5 âncoras, mas com uma só global, que utiliza os recursos dos 5 RIRs além de outros recursos reservados, recursos de endereços de IPS destinados a usos específicos.

O bom é que isso se pode configurar de maneira individual, ou seja, que uma parte que depende de uma só âncora, de um RIR, pode ser ativada dessa maneira, ou não.

Ouvi que falaram em regulação e como isso pode ajudar. Há um passo antes da regulação do do ponto de vista da influência e da incidência. Muitos governos são usuários das tecnologias ICT. Vocês tem as suas próprias redes e os seus próprios sistemas. Porque vocês querem que fornecedor de serviço que tenham roteamento seguro e como cliente deveriam pedir que façam. Essa é uma boa maneira de divulgar o interesse nessas implementações dessas tecnologias. E não quero emitir esse passo intermediário, em que vocês como usuários das ICT podem também demander qualidade dos seus fornecedores de serviço, pedindo que utilizem roteamento seguro.

PRESIDENTE DRYDEN: Obrigada. Passo a palavra para Malásia.

MALÁSIA: Obrigado, Presidente. Obrigado por apresentar essa tecnologia. Queria dizer que nesse momento temos muitos desafios para promover o

DNSSEC e os nossos ISPs. Apesar de que nós os regulamos queremos que se ofereçam como voluntários porque vocês devem entender que a atualização é muito lenta.

Me interessa muito os prazos e os programas de extensão, para que possamos promover essas tecnologias nos nossos países e em nossos ISPs.

PRESIDENTE DRYDEN: Adiel, quer responder?

ADIEL AKPLOGAN: Quanto as prazos estamos trabalhando em conjunto para poder ter os mesmos prazos e avançar nesse sentido. Estamos pensando em lancer a plataforma, para que existam os certificados e que se possam assinar. Então o sistema já está em andamento, pode ser utilizado. O objetivo da apresentação hoje é gerar essa consciência para o GAC, de maneira que vocês podem gerar a mesma consciência localmente, que se comece a usar o sistema.

Também temos um bom enfoque dos fornecedores que tem integrada essa tecnologia IOS. Quer dizer que pode já ser usado no mundo real de internet. A atualização vai ser lenta, logicamente, mas já está ali e certamente vamos começar a fazer com que as pessoas utilizem também. Obrigado.

PRESIDENTE DRYDEN: Adiel, obrigada por essa resposta. Temos a Comissão Européia, Uruguai, Reino Unido e depois fechamos.

COMISSÃO EUROPÉIA: Obrigado, Presidente. Eu queria agradecer também os apresentadores, não só por estarem aqui, mas por fazer que essa tecnologia seja compreensível para todos. Entendemos que não é fácil e por isso agradecemos.

Tenho duas perguntas que pode ser respondida por qualquer um de vocês. Quanto às âncoras da confiança. Só nos referimos aos registros de internet, ou a outros que podem ser âncoras confiáveis no sistema?Há um requisito especial para que uma entidade possa perguntar esse serviço e ser confiável nos operadores?

E a segunda pergunta. No início da apresentação foi mencionado isto, por isso talvez não entendi, ou não lembro bem. Escutei alguém que se referia ao fato de que a comunidade tem inquietações interrogantes sobre a que se tome uma decisão que envolva a revogação do certificado digital, utilizando o sistema de RPKI. Queria saber se vocês podem explicar que partes da comunidade estão tendo essas dúvidas, essas preocupações e se houve casos de rejeição, ou se isso poderia acontecer a curto prazo.

Como Comissão Européia, não vamos fazer nenhum comentário sobre o que fazem ou não as comunidades locais. Mas queremos saber se isso já acontece ou é uma preocupação hipotética, como aquelas que nós, como autoridades públicas geralmente acusamos de colocar na mesa, e por isso, agradeço pelo esclarecimento.

GEOFF HUSTON: Quem pode ser uma âncora confiável? Vamos recuar e fazer uma pergunta mais básica. Quem pode emitir certificados que demonstrem que alguma das partes tem um recurso? Em teoria qualquer pessoa podia fazer, mas temos que acreditar. A parte que emitiu os recursos, talvez a melhor parte, é a que pode emitir o certificado. Por isso se APNIC gera um bloco de endereços, para um registro de internet local, então o certificado que emite APNIC é aquele que se deve confiar, em lugar de outro que não se deve confiar.

O modelo de confiança foi alinhado precisamente, com o modelo de atribuição de endereços e na medida, em que haja sistemas seguros, as pessoas que usam vão poder escolher qualquer um dos modelos de confiança. Nós vamos recomendar que utilizem o conjunto de confiança que corresponde as agências que alocam os recursos, que se trate de um conjunto de confiança de materiais emitidos por qualquer um dos cinco RIRs, e são 5 modelos de confiança, ou que a gente utilize uma entidade de confiança para descrever a raiz de IANA. Isso depende de vocês. Mas talvez não seria inteligente replicas o que nós fizemos nos navegadores, porque tivemos mais de 100 entidades e nesse caso são demais. Então talvez um número menor, seja melhor, mas não tem que ser apenas um.

Quanto a segunda pergunta em relação as discussões das preocupações, acho que se deve informar que essas preocupações tinham mais a ver com a área européia e se deve discutir nos foruns adequados. Infelizmente Axel não está ali, mas houve instâncias em que no espaço diferente, por motivos diferentes, houve ordens de revogação de certificados por outros objetivos que tiveram os tribunais. Então podemos aplicar também isto aos certificados digitais?

Queríamos pensar que não, porque os certificados são o espelho do conteúdo do registro subjacente e, revogar um certificado não muda o registro per se, mas eu não estou muito certo se isso foi o que aconteceu.

Quero pensar que na medida em que estamos avançando nesse processo e entendemos mais integração do certificado e a criptografia digital nessa infra-estrutura o risco de que a sociedade, instituições e ferramentas funcionem com isso e agradeçam seus próprias problemas e responsabilidades sobre isso, a revogação não vai ajudar em nada.

PRESIDENTE DRYDEN: Geoff, obrigada pela apresentação.

URUGUAI: Não sei se perdi mas queria entender como essa infra-estrutura se relaciona, com a infra-estrutura nacional pública. Não apenas do ponto de vista técnico, mas também legal. Vocês sabem que em cada país o valor legal de um certificado e da confiança do sistema da infra-estrutura, se relaciona com partes, com autoridades de autenticação que tem o poder de emitir o certificado por uma entidade regulatória. Quer dizer que a infra-estrutura pública nacional está vinculada com algum tipo de adequação e quero saber como isso se relaciona, se existe algum tipo de compatibilidade ou não.

JOHN CURRAN: Está fazendo uma pergunta legal e não sou advogado. Tendo dito isso no processo de explorer os aspectos de oferecer certificados RPKI

parece ser que cada país tem seu próprio marco para validade legal de um document assinado de maneira digital. Isso significa que os RIRs ao emitirem esse certificado, ficamos certos de que se saiba o significado desse certicado. Ou seja, estamos falando do detentor de um recurso, que que considera esse detentor. Qual considera a entidade que pode fazer o roteamento desses endereços. Por isso e que em alguns países as jurisdições nacionais é que fazem esse certificados e os tornam equivalentes a documentos assinados emitidos pelo registro. Isto tem questões para aqueles que envolvem esses registros que tenhamos cuidado ao fazer rodar esse certificado. Mas isto é uma situação que se gera país a país. Não posso dar uma resposta geral, mas posso dizer que os fornecedores de países que emitem esses certificados, tem que poder entender que estão emitindo documentos com a mesma fortaleza legal.

URUGUAI: Se o ISP tem alguma responsabilidade legal por cometer um delito, como um ISP, o marco legal em que estaríamos trabalhando é o marco nacional. E esse marco legal está regulamento por essas leis nacionais e elas tem a sua infra-estrutura nacional. Para uma das perguntas, o que pode fazer o GAC para resolver isso? Talvez ter certa compatibilidade entre o marco nacional, para poder organizar o trabalho dos ISPs no nível local. Mas acho que temos que ter mais informação de vocês para saber como trabalhar nos nossos próprios países.

PRESIDENTE DRYDEN: Raul, por favor.

RAUL ECHEBERRIA: Quanto a arin, essa é uma infra-estrutura separada. Quanto aos certificados que são emitidos com esse marco, com esse contexto, tem o único objetivo de ser utilizados para o roteamento, de maneira que não vai haver nenhuma transação no uso desses certificados. Os ISPs não vão usar esses certificados para fazer transações de nenhum tipo local. Por isso não vai haver responsabilidade legal nesse sentido. Vão usar essa informação apenas para saber se a rede que está anunciando um bloco de endereços de internet é quem tem autoriadade para fazê-lo ou não. Vai permitir que se tome decisão sobre roteamento ou mais nda. É por isso que esses certificados não vão ser utilizados em nenhum país,para nenhum objetivo que esteja regulamentado sobre o marco legal de cada um dos países. Não sei se responde a pergunta.

URUGUAI: No caso que o ISP não utilize corretamente o roteador para utilizar a rede em realidade.

GEOFF HUSTON: Há muitos tipos de certificados. Alguns são utilizados nos sistemas de nomes de domínio para os websites HTTP e outros são utilizados para demonstrar identidades dos cidadãos de um país. Convencionalmente nos encontramos com que os certificados que tem um interesse nacional regulatório são certificados que demonstram a identidade e o papel das pessoas, mas eles podem fazer muito mais do que isso e aqueles que nós trabalhamos são muito mais similares aos que são usados no sistema de nomes de domínio, quanto a associação de um nome de domínio a um endereço de IP para os websites seguros. Convencionalmente esses certificados que caem diretamente no marco

regulatório legal per se, de forma convencional e muitos marcos, tem mais vinculação com as práticas nacionais da indústria.

Diríamos que esses certificados que não demonstram identidade, não demonstram o papel, mas que associam um par de senhas, tem uma reflexão de um artefacto técnico que é diferente de um papel e por isso, tem mais a ver com a área regulatória que fala sobre artefactos técnicos e questões técnicas como certificados de nomes de domínio, o que são diferentes dos certificados de papel ou de identidade. Não vejo o nível de interesse regulatório nesse sentido, como acontece em outros tipos de certificações.

PRESIDENTE DRYDEN: Vamos ter que passar para o último palestrante. Espero que essa troca possa continuar online e possamos falar no futuro com vocês no GAC. Agora tem a palavra Reino Unido e depois fechamos a sessão.

REINO UNIDO: Obrigado, Presidente. É muito útil e complementa a informação que recebemos da Europa pelos governos europeus. Também o que disse o RIPE NCC, nos lembra que o roteamento seguro continua sendo o nosso objetivo para a comunidade. Esperamos que esse alvo possa ser atingido e conforme lembro dos relatórios que recebemos, os relatórios europeus que recebemos, era aparente que nem toda indústria estava em linha, pelo menos pelas respostas que escutei. Estamos falando dos ISPs, claro. Para nós, nos governos temos que continuar vendo que a indústria não está falando apenas com uma voz e quando se trata do que podemos fazer para promover a conscientização, é como que

temos uma mão amarrada e dizemos para a indústria, olha temos que encontrar uma forma de avançar. Aí aparece RIPE NCC e nos apresenta o trabalho que vai nessa área e quais são os relatórios. Com certeza que vamos ter mais informação em Amsterdã, quando os governos se reúnam e espero que possamos ter outros RIRs que também forneçam informação. No ministério onde eu lidero a assessoria técnica, os pontos técnicos, quero dizer algo, fazer algumas pergunta básicas, não técnicas.

Primeiro se a expansão do sistema de nome de domínio que tem milhares de gTLDs possíveis para os próximos 10 anos e que vai permitir acrescentar mais urgência a esses trabalhos. Essa seria a primeira pergunta e a segunda é porque a implementação do RPKI não vai ter uma consequência significativa no abuso de DNS. Obrigado.

GEOFF HUSTON: A pergunta é simples, a resposta não. Os nomes e os números funcionam de forma separada, no caso e a expansão do espaço de nome na estrutura de nomes dos novos gTLDs não tem qualquer vinculação com esse recurso de RPKI. São completamente separados e não tem qualquer relação.

O tema do escalamento da insegurança na internet é uma questão interessante. Há 15, 20 anos, insegurança era o produto de uma criança de 16 anos, que não tinha o que fazer pela tarde e quando vemos agora a questão da insegurança, se tornou uma indústria. Uma indústria criminal, mas finalmente uma indústria. E certamente qual é o valor das transações da internet, subverter a operação normal de internet é uma coisa que se torna de interesse aos jogadores que não querem jogar e que não merecem a nossa confiança. Atacar o roteamento é uma coisa

que pode ser feita com recursos e conhecimento e que pode ser um ataque muito efetivo. Pode se atacar a ppntos específicos na rede ou se pode ampliar o efeito de um ataque. Essa não é uma situação confortável e certamente a medida para assegurar o roteamento que não é que não se faz porque não temos o que fazer na próxima semana, na quarta-feira. Simplesmente, porque temos uma agenda que nos pressiona muito que tem a ver com a segurança.

A estrutura na segurança é o pior dos problemas que podemos ter. Todas as outras coisas podem funcionar, mas a infra-estrutura, se o triângulo vai a direção incorreta o triângulo funciona de todas as formas ou avança de todas as formas. Estamos vendo uma implementação como fator de mitigação das questões potenciais, sob as quais pode ser subvertida a internet. Qual é o efeito da base criminal ou outra forma de criminiliadade que não merecem a nossa confiança. Então sim, é importante.

PRESIDNENTE DRYDEN: Eu quero agradecer como sempre ao NRO por apresenter esse ponto, esse tema. Houve outro nível de interesse, portanto não queria evitar que continuasse o debate. Espero que possamos continuar ou abordar esse tema outra vez no futuro e agradeço novamente a todos.

Para o GAC nós não nos beneficiamos quando temos almoço muito curto, por isso vou sugerir continuar 14h45 e depois vamos continuar com a nossa agenda.

Então 14h45 vamos continuar. Obrigada.