BUENOS AIRES - DNSSEC para Todos
Segunda-feira 18 novembro, 2013 - 17:00-18:30
ICANN - Buenos Aires, Argentina

JULIE HEDLUND: Quero dar as boas vindas a todos aos DNSSEC, que um guia para os principiantes à medida que vão entrando, por favor. Tomem lugar, sentem ao redor da mesa, para participar de uma maneira mais, numa maravilhosa actividade, vai ser muito divertido por favor, sentem-se aqui na mesa, vamos começar em alguns minutos, estamos resolver um problema técnico com a camara o que vamos fazer é começar com a primeira parte em breve vou mostrar os slides e depois, vamos continuar.

PRESENTER: Estamos aqui então, estamos prestes a começar íamos filmar isto com a camara mas vou deixar isto de lado, estamos com problemas técnicos, a questão da camara está relacionado com um DNSSEC que algumas questões são complexas.

À sessão de DNSSEC para todos e também para principiantes, esta questão do DNSSEC, pode ser algo que cause um pouco de medo no início e há palavras cruciais, não vamos sair daqui especialistas em DNSSEC, mas vamos dar uma introdução geral, para utilizar no DNSSEC vocês vão conhecer algumas palavras cruciais e as pessoas vão levar vocês mais a sério a partir disso.

Eu gostaria de apresentar algumas pessoas que vão participar. Nesse

grupo temos o Russ Mundy, que é o pesquisador de Parsons, Russ também dirige as ferramentas do DNSSEC que trabalha à muito tempo já organizou muitos Workshops e ao lado dele está Roy Arents. Olá Roy. É Roy é bolsista de Nominet, que é o registro de ".UK" também ele nos ajudou com algumas especificações da DNSSEC, também agora, quero apresentar a Julie, dá para escutar, dá para escutar melhor, tão-me escutando, agora sim, muito bem, depois temos aqui Julie, a Julia nos ajuda a organizar isto e nos manter um pouco mais, Norm, é o director de inteligência da DNSSEC mas Crowdstride é uma companhia de segurança cibernética. Jaques trabalhar para SIRA, que é o registro de ". CA", e esses são, acho que somos só, mas há alguém mais que eu não nomeei.

Quantos de vocês sabe alguma coisa sobre o DNS? Levantei o braço por favor, e quantos sabem alguma coisa sobre o DNSSEC?

Bem, é, lamento informar que vocês sabem do DNSSEC é porque está incorrecto provavelmente vocês acham que foi inventado há poucos anos, na verdade foi inventado à 7000mil anos, na verdade, e foi inventado por um grupo de homens das cavernas. E esta é uma deles, chamo-lhe a mulher das Cavernas, chamávamos-lhe de Ogwina. Ela está olhando, no Grande Canyon, aqui temos outros, a Og,outro inventor, está olhando do outro lado do Grande Canyon, Então a Ogwiana e Og, digamos, estão tendo, algum, estão-se olhando de alguma maneira maliciosa, então é muito difícil para, ter que, subir e descer, o grande Canyon, de subir e descer o grande Canyon, várias vezes e é um pouco difícil para eles poderem estar mais perto, e numa dessas visitas enquanto eles estão-se olhando, eles se dão conta, que há fumaça

saindo dessa fogueira que eles fizeram, então se dão conta que podem usar então sinais de fumaça, e se dão conta que podem tirar esses sinais para poderem-se comunicar e podem então enviar cartas de amor de um lado para o outro.

Então, podem avisar quando querem almoçar juntos etc. depois um dia parece, outro homem da caverna, caminhos que então pensa que é divertido mandar mensagens, entre as mensagens, entre, e caminhos então, começam a falar de bananas de qualquer coisa que não tem nada a ver, ele se intromete no meio da comunicação entre eles, e ela fica meio confundida e não entende quais são as mensagens correctas, e quais são os inventados por Kaminski.

Então ela fica um pouco chateada, com tudo isso, desce do grande Canyon, caminha então durante 4 dias, e Gweniogy para procurar resolver o que devem fazer, então eles acodem às pessoas mais idosas da dessa comunidade e perguntam sem que Kaminski se meta no meio um deles, é um homem das cavernas chamado Diffy. Ele acha e reflexa no problema e termina tendo uma ideia brilhante, ele se levanta, corre até a caverna do Og, e atrás da caverna há uma areia muito, especial e o que torna isso especial é o facto de só encontrada na caverna de Og. Diffy então retira, tira um pouco desse punhado de areia, e atira para a fogueira de Og, que tem essa cor brilhante azul, então a Ogwina e Og, podem continuar conversando contentes, Ogwina sabe tudo o que deve fazer, é somente olhar os sinais azuis porque o Og pode ter, e tem, esta cor azul, e Kaminski pode enviar mensagem e ela vai ignorar.

Então, podemos então tirar uma conclusão disso o que faz o DNSSEC como essa fumaça azul para o DNS, é uma forma então, o receptor pode

saber que recebeu a mensagem e a pessoa que, so apena uma pessoa pode enviar essa, essa fumaça azul para saber quais são as mensagens correctas e quais não.

Depois disso então passo a palavra a Roy que vai dar uma representação, uma apresentação, sobre o DNSSEC.

ROY ARENS: Olá! Eu sou o Roy Arens. Vou comentar sobre o DNSSEC, eu vou, eu gostaria, vou fazer uma pergunta e quero, quem entende que temos servidores raiz no mundo, por favor levante o braço. Quem sabe então, como funciona o DNS, vamos então, primeiro slide por favor.

Basicamente, isto basicamente, é a árvore desse padrão, a raiz é em cima, e a raiz então delega o seu, é aqui a Argentina por exemplo, e a ".ar" etc. etc.

Um, Um, o resolutor da companhia sabe onde estão os servidores de raiz, os seus vários, vou apresentar depois, eu usuário não tenho ideia de como é o DNS, por exemplo de um somente pode falar com ISP, ele vai da raiz para, níveis mais baixos, por exemplo *Bigbank.com*, e tem o endereço, o resolutor tem a, então ela é, ela é verificada, para ser usada futuramente. Neste momento, gostaria de mostrar como realmente trabalhamos com o DNS, este então é um pequeno jogo, temos aqui vários jogadores, esse slide vimos antes, vocês aqui têm os servidores de raiz ou *ponto.com*, têm, enquanto a equipa está preparando digamos, todo o material necessário, eu vou apresentar Joe. Veja o usuário típico como exemplo, está sentado com o seu sistema e sua

casa com o seu laptop, procurando navegar e procurando então digitar algo na barra de endereços do navegador. E o que eu vou mostrar aqui para vocês normalmente ocorre basicamente depois de vocês digitam e colocam entre o, querem um acesso de domínio e antes de chegar à pagina que vocês querem.

Isto ocorre em, em, pouquíssimos segundos. Para ser honesto, isto ocorre com computadores e com sistemas, não com pessoas. Como é o exemplo que eu tenho aqui com pessoas. Temos Joe, hoje como utilizador, Alan, temos também aqui o nosso ISP aqui, o servidor raiz, aqui, eu sou ".com". Esse é o *bigbang.com*, que você verá aqui então, como um resolutor funciona. Vou passar então o microfone para Jaques Latour.

JOE UTILIZADOR: Muito bem, sou o Joe o utilizador, fazendo um pagamento através da internet. A única coisa que consigo devo pagar as minhas contas. E através da internet eu me sinto no computador e escrevo www.

ISP: Obrigado. Sou o ISP e a única coisa que eu sei é onde está a raiz. È a única coisa que eu tenho que saber, sou programado para isso, não sei onde está o banco e vou perguntar ao então ao servidor da raiz. "Sabes onde está o bigbank.com?".

ROOT: Não sei onde está, sei ou que é *ponto.com*, aqui por exemplo 1.1.1.1,

ISP: Obrigado. "Olá ponto.com, estou procurando o *bigbank.com*, você sabe onde o posso encontrar?".

.COM: Não. Não sei onde está o *www.com*. Mas sei onde está *bigbank.com*, ele mora no tal endereço 2.2.2.2. Esse é o seu endereço".

ISP: Olá *bigbank* procuramos *www.bigbank.com*.

BIGBANK: Sim, na verdade eu sei onde está o *www*, está em 2.2.2.3.

ISP: Muito obrigado". "Olá! Joe, então o endereço é este 2.2.2.3.

JOE UTILIZADOR: Muito bem, Então eu escrevo no teclado o endereço do meu banco e eu tenho um ISP que me dá um número e eu vou então poder aceder a esse endereço. Bom é um pouco mais rápido na vida real, mas é assim que funciona o DNS. Esta é a base da transacção. Então foi colocada, vocês podem ver, na barrinha deles. Preciso da minha resposta Muito bem. Agora o que nós vamos fazer é mostrar a vocês como podemos ver uma pessoa então que chega para atacar. Esse então vocês vão ver

aqui, então, como ocorre um ataque no DNSSEC. Vamos então com o mesmo cenário, com a pessoa que vai atacar, então, o nosso meio. Eu vou-me sentar, vou apagar minhas contas, msmsm, coloco aqui então o endereço que eu tenho do *bigbank.com*.

ISP: Obrigado. Vamos ver então Você que chegará até ao *bigbank*, tem um primeiro, tem que ir ao servidor raiz, pergunta a ele, vai dizer onde está o bigbank.com.

ROOT: Não Sei, não sei onde está *www*". *www.com* está em 1.1.1.1. Olá! Senhor 1.1.1.1, *www.bigbank.com?*

.COM: Não sei onde está esse endereço. Mas sei onde está bigbank.com ele mora no endereço 2.2.2.2".

ISP: Olá! bigbank estou procurando www.bigbank.com. Você tem o endereço IP?!.

DR.EVIL: Sim, eu tenho. è o endereço é este 6.6.6.6."

ISP: Muito bem! Optimo. Muito Obrigado". Olá Joe. Aqui tem o endereço que Você estava procurando, Você pode se conectar para fazer todos os seus pagamentos *online*, pagamento dos bancos.

JOE UTILIZADOR: Muito bem! Novamente, eu acho que me vou dirigir até *bigbank.com*, esse monstro desse doutor, ele se apossou de mim. Todas as minhas transacções vão ir para o doutor, ao bandido. Vão chegar até á sua conta. O que aconteceu aqui, é como funciona o DNS para DNSSEC. Há um ataque no meio e isto ocorre, e ocorre com os bancos de grande porte. O problema é que não há elementos e conhecimento entre os diferentes servidores. E a hierarquia eles não compartilham informações. Não conversam entre si, nem sequer eles se conhecem. Então, faremos lembrar que aqui é aquela história da fumaça, de um conceito chamado cadeia de confiança. E aí é onde, ou seja é autorizado, a compartilha de informações e chaves, e sempre como uma fumaça, para compartia, para trocar informações. Devemos passar pela cadeia de confiança.

ROY ARENS: Antes de passar então, quero contar outra coisa, Você s lembram-se da imagem onde tínhamos, ou OGIWA á esquerda falando com Og. Então DNS a esquerda está essa linda mulher OGIWA. OGIWA é uma mulher moderna que estava falando somente com OG o servidor, mas muitos diferentes servidores. O próximo slide por favor. Como vocês já sabem a OGIWA, não sabe realmente quem é OG. Ele não sabe que é o servidor que tem toda essa informação que vai e vem de um lado para o outro.

Pode ter sido alterada com DNSSEC e vou mostrar então, a OGIWA pode decidir entre um OG falso e uma informação falsa. E um OG real fazendo isso então com a Fumaça sul, um DNSSEC e com as assinaturas digitais e etc. No DNS não há segurança. Esse protocolo foi inventado há em 1992 ou 1993, muito antes de existir a internet. Neste momento muitos pesquisadores em rede se juntaram, se reuniram, e ninguém pensou que isso poderia ser atacado com abusos. Como por exemplo os homens podem ser alterados facilmente e as pessoas podem então entrar e poder invadir informação e terminam envenenando a cache. Vamos fazer novamente outra representação. Temos a raiz "COM", com original bigbank.com, á esquerda, e o falso á esquerda em vermelho. Então é o bandido o vermelho. Como fazemos isso com um DNSSEC. Utiliza um conceito de assinatura digitais basicamente. São criadas algumas chaves onde há uma chave pública e outra privada. A pública vocês podem fornecer para qualquer pessoa, a chave privada deve ser guardada num lugar muito seguro, A chave pública é uma quantidade de bits que vocês podem guardar qualquer DNS ou endereço, por exemplo. Vocês podem então escrever a chave, essa então é uma chave pública e é guardada no DNS. Quando vocês assinam o DNSSEC é criada então a assinatura fazendo isso, através de uma chave privada que valida essa assinatura. Não são mais que uma serie de bits. Que Você também pode ter no DNS, que é feita a chave no DNS e também temos as assinaturas no DNS. Então deve haver uma ligação entre todos esses componentes com a raiz ".COM", *bigbank.com* e basicamente para juntar tudo isto, da raiz e a raiz e o *bigbank*. A solução que nós achavamos de registo de DNS é uma versão simplificada da chave DNS. A raiz DNS o que todos possuem deve haver um resolutor para confiar nessa informação. já que o resolutor confia na raiz, aí então vai validar a

informação recebida. O resolutor pode então confiar no ponto.com,também. Então com esta informação, o resolutor então começa a confiar no *bigbank.com* e assim por diante. Com esse mesmo conceito de alto nível, como assinamos toda essa informação de acesso á cadeia de confiança desde a raiz até ao ponto.com para o bigbank.com. podemos distinguir então de forma adequada, entre a informação falsa que não pode ser assinada porque a pessoa que ataca não tem a chave privada que tem o bigbank.com. O resolutor então pode distinguir entre uma informação assinada adequadamente e uma informação não assinada ou assinada de uma forma enganosa. Então vamos fazer essa representação com DNSSEC. Vamos aplicar então agora com esse outro cenário. Vou convidar então os meus amigos.

ROOT: Olá! Sou a raiz e antes de mais nada a raiz deve estar assinada então eu vou fazer um assinatura em mim mesmo. " Essa é a minha chave. Agora devo trocar chaves com *ponto.com*. Olá *ponto.com* o senhor realmente é ponto.com?

.COM: Sim eu sou o *ponto.com*.

ROOT: Nesse caso temos que trocar de chaves.

ROY ARENS: O que acabamos de fazer vamos fazer outra fez.

.COM: Eu sou o ponto.com posso confiar em você, em que você é realmente o *bigbank.com*.

BIGBANK.COM: Sim perfeitamente.

.COM: Então o senhor, eu quero dar isto ao senhor. Porque o senhor merece.

ISP: E agora todos estão aqui na minha zona de assinados e o endereço *www.bigbank.com* está assinada.

JOE UTILIZADOR: Agora então vamos fazer a transacção do DNS. Novamente temos um ataque, mas desta vez temos o DNSSEC que vai nos proteger. A mesma transacção mas que é de contas a pagar. Ai como eu gasto dinheiro tão rápido. Porque vai este senhor que é malvado. Esse malvado *www.bigbank.com*.

ISP: Obrigado. O senhor quer ir até ao bigbank.com. Sim eu vou fazer uma

consulta primeiro. Preciso de falar com o servidor raiz. Então temos a chave publica e sei qual é. Que é esta que está na raiz. Muito bem o senhor que é a raiz, o senhor sabe onde fica *bigbank.com*.

ROOT: Sim, bigbank.com está no seguinte endereço 1.1.1.1. Espere um minuto que eu vou assinar.

ISP: Bem, vou verificar a sua assinatura, esta assinatura coincide com a chave. Então vou me dirigir até ao 1.1.1.1.

ROOT: A chave é um numero realmente longo.

ISP: Ola 1.1.1.1 quero ir até *www.bigbank.com*.

.COM: Não sei onde está esse endereço bigbank.com mas sei onde está o *www.bigbank.com*, ele fica no seguinte endereço 2.2.2.2 e Você tem a assinatura primária a chave para o bigbank.com.

ISP: Vamos ver a assinatura, vamos ver se a chave está correcta. Sim,

coincide. Agora então vou perguntar ao bigbank.com pelo endereço do www.com.

DR.EVIL: A resposta é 6.6.6.6.

ISP: Muito obrigado. Vou verificar com a chave. A chave não está correcta. Por favor vai embora. Muito obrigado.

BIGBANK: Então o endereço é 2.2.2.3. E está neste site.

ISP: Esta verificado correcto, muito obrigado. Ola senhor Joe, aqui tem o endereço 2.2.2.2 e a assinatura pode ser validada.

JOE UTILIZADOR: Muito bem senhor ISP. Agora está tudo validado e esse numero então foi confirmado. E é como funciona a transacção. Vocês devem levar em conta que o comum utilizador, como qualquer utilizador, não vez nada. Sempre faz a mesma consulta e o resto corre entre o ISP o resolutor e os registradores e os registos, Isso não ocorre no nível dos utilizadores. Obrigado. O doutro malvado está aqui mais uma vez.

PRESENTER: Ok. Muito bem. Obrigado. Queremos fazer que seja o mais divertido possível. Que seja a sessão mais divertida da semana. Vamos ver se conseguimos mais. Tomara que sim. Na verdade queremos ser informais. Ainda não houve perguntas, mas esta é uma sessão muito informal. Então tudo o que as respostas que sejam necessárias é só levantar a mão e abordaremos todas as consultas. A minha parte, aqui da minha apresentação, desta sessão, tem a ver com duas coisas. Na verdade dar exemplos mais específicos de uma substituição de identidade.

JAQUES LATOUR: Eu tenho na verdade uma pergunta, sobre a peça que vocês fizeram, a representação, Há uma pessoa que tem uma francês muito interessante muito pronunciado que faz também em inglês. È o caso por exemplo, vocês deviam utilizar o inglês para o DNSSEC ou também isso pode ser aplicado às cadeias de caracteres internacionalizadas?

ROY ARENS: Isso se aplica a tudo o que está escondido no DNS. O *IDN data* então do ponto de vista do DNS é o seguinte. È assim. Muito bem. Vamos passar então para o seguinte slide. Sobre o DNSSEC. E porque poderíamos ficar preocupados pelo DNS? O DNS contem os conteúdos DNS, eles devem chegar correctamente às solicitações. Porque senão vai haver problemas. E a aplicação do OGWIA final, que mais nos preocupa. Porque os OG final pensa que o DNS tem verificado os nomes. Mas a infraestrutura da rede por todo e a mecânica utiliza endereços de IP. De algo modo, então a tradução deve ser feita corretamente e é aí então

onde os delitos, os ataques, acontecem. Onde o *hijacking*, acontecem. Para os mecanismos que se produzem aqui, Depois vamos escrever o que o sequestro de identidade. Quando temos um sequestro no DNS não é porque a gente quer sequestrar, digamos, o DNS. Não é porque ninguém se importe com o DNS, p DNS é importante mas para as pessoas que trabalham na internet o que importa são os aplicativos. Um dos pontos que me surpreende aconteceu faz uns 5 anos. Existe um *software* que permite fazer o *hijacking* do DNS, o sequestro. Porque é necessário, ou era, pelo menos necessário um certo software para que os estudantes fizessem esse tipo de actividade, sequestro., *hijacking*. Não sei se utilizam agora esse tipo de coisas, mas para mim não foi muito feliz o facto de que isso, esse *hijacking*, então há muitos códigos e muitas coisas, que os estudantes podem fazer, porque pedimos para eles. Que eles façam. Então, quando o DNS se é utilizado e o DNSSEC no website, é possivel utilizar a informação que faz parte do protocolo para fazer coisas, como por exemplo, para encaminhar se as pessoas estão vendo ou não, e utilizado o DNSSEC quando a pessoa tem acesso a um website. Não é muito frequente mas alguns sites fazem e á projectos que têm esse tipo de capacidade. Então o que nós fizemos foi modificar termos parte do nosso website, para que podessemos mostrar de forma real uma situação de apropriação ou de *hijacking* do website. Vamos ver como isso acontece, que é diferente mas, basicamente acontece de modo similar aquilo que aconteceu na nossa peça de teatro. O que acontece que o usuário envia a consulta para um ISP local ou resolutor e ele começa, e vai e vem em toda a rede. Por último a consulta volta para o usuário. Quando essa resposta volta, ele pode falar com o banco, mas a solicitação tem a ver com isso. Mas não é completa, até que nos chegue a resposta final, por parte do DNS. Então quando temos um

buscador com DNSSEC, podemos ver na parte superior, se o DNSSEC tem algum marca é activado, isso pode ser detectado observando as consultas ou *queries* que vão no DNS. Que tem a capacidade de DNSSEC. Então vamos colocar, vamos riscar aqui DNS se o buscador não tiver DNS, digamos que não haverá DNSSEC, isso significa que estamos numa página com ou sem DNSSEC. Equivalente ao doutor Malvado e o nosso doutor malvado *hijacking* ou de apropriação de identidade. Aqui o usuário acede, o doutor malvado também pode aceder a essa informação, e ele vê qual a solicitação e o que ele faz, Dr.EVIL *hijacking*, ele pega a resposta e responde para o usuário antes da chegada da resposta real. Porque, como podem ver nessa imagem, a resposta real chega muito depois, é muito mais lenta do que a resposta falsa. Agora se estamos utilizando DNSSEC o que acontece é o seguinte. O usuário pode detectar que a resposta que obtém do doutor malvado não é válida. Então ignora a resposta. E vai obter então a resposta correcta da localização real dessa resposta que vem ou não do DNSSEC. Depois irá para o servidor e entra no servidor que ele escolhe. Esta é uma forma diferente de mostrar o que acabamos de ver na peça de teatro. Se colocássemos todos os exemplos, porque se não esse slide seria bastante extenso. Perguntas?

HOSAM HASSAN: Sou HOSAM HASSAN eu tenho uma pergunta. Mas eu acho que já responderam. Essa pergunta tem a ver com o DNS.

ROY ARENS: Mais perto do microfone, por favor.

HOSAM HASSAN: O DNSSEC cria uma confiança entre a raiz e os outros domínios de alto nível, de primeiro nível, por exemplo os ponto.com e outros nomes de domínio. Mas se houver um caso de sequestro, ou *hijacking,* isso afecta o ISP ou o usuário final, que está no DNS. Porque, do meu ponto de vista, o resolutor tem endereços que consultam o servidor. Então se a substituição ou delete acontece nesse nível, isso vai derivar em encaminhar o trafego para um outro servidor raiz. Então, nada vai acontecer. Não tem a ver com isso, está entendendo a pergunta?

ROY ARENS: Eu entendo a sua pergunta. A raiz tem operador de resolutor que está trabalhando em uma raiz diferente que não foi assinada pelo DNSSEC,

HOSAM HASSAN: Vimos que a relação de confiança entre os domínios, a raiz e o resolutor. Onde acontece a apropriação. Sobre o ISP. Antes de sair para a raiz.

ROY ARENS: Então se a consulta fica modificada.

HOSAM HASSAN: No resolutor do ISP, e para ir para o endereço de IP que estão por fora do servidor em outros servidores. Isso então sairia do ecossistema

principal. Porque iria parar em algum outro servidor que poderia conter uma outra base de dados de um outro servidor raiz.

ROY ARENS: Passamos a palavra para o Ray.

RUSS MUNDY: Vou repetir a pergunta. Eu acho que entendi. E me desculpe se não entendi, porque estava bem entendido. O que eu entendi é o seguinte. O que é que acontece se a raiz e o resolutor estão comprometidos de tal modo que os endereços de IP são trocados e apontam para um conjunto de servidores totalmente diferentes, é isso? Então a resposta seria. Se a raiz fica comprometida e o resolutor ainda pode continuar fazendo a validação, porque tem a chave do DNS, então tentará validar a informação que vem da raiz. Se houver uma raiz alternativa a informação, obviamente, estará errada. Isso vai significar que a informação não vai chegar no usuário final.

HOSAM HASSAN:: Não, porque a apropriação acontece no resolutor do ISP antes da activação. A relação entre o servidor raiz e o domínio de alto nível. Mas a apropriação acontece ao nível do ISP, porque aponta a uma outra base de dados. A um servidor por fora do DNS. Por fora do alcance da abrangência vai para um outro sistema para uma outra base de dados. Então, Nessa etapa o DNS intervém está apontando com um *click*, em locar de apontar esse.sec.sec, esta apontando para outro lugar.

RUSS MUNDY: Então vamos *graficar*. Estamos aqui em cima e o usuário envia a consulta para esse ISP. Se há uma parte da maquinaria do DNS mudar ou se estiver significativamente comprometido, porque há um *software* de segurança que não está a ser executado correctamente, os resolutores são totalmente imprevisíveis, Qualquer coisa pode mudar qualquer coisa, então devemos ter confiança em que o ISP está a funcionar correctamente ou não. E ter também, o facto de ter confiança numa operação posicional em que deve funcionar de modo correcto. O DNSSEC não pode garantir que esse computador, não pode garantir os requisitos físicos do computador. Mas esses requisitos devem existir e devem ser respeitados para que o DNSSEC possa funcionar.

WARREN KUMARI: Warren Kumari, da Google. Se você não confia nos resolutores dos ISP, se eles não são confiáveis e mentem, para você exige que uma serie de pessoas Que desenvolvem software para que possam ter o seu próprio resolutor de uma forma local no seu próprio computador.

HOSAM HASSAN: O usuário afinal pode utilizar isso sem necessidade em que se utilize outro ISP, pode ter um resolutor.

WARREN KUMARI:: Tê-lo em uma máquina, é uma boa ideia, Que Você tem no seu próprio computador e não deve depender de mais ninguém.

RUSS MUNDY: Se temos em conta esse desenho que, vemos que estamos fazendo a validação. São muitas as pessoas aqui sentadas que tem isso implementado ou implementaram nos computadores. É fundamental confiar no ISP. Poderemos fazer de modo mais rápido, confiando no ISP, por muitos motivos. Então, ter operações seguras é importante, mas também não é essencial para o sucesso do DNSSEC. Não sei se isso responde á pergunta. Isso responde à sua pergunta?

WARREN KUMARI: Na realidade eu ainda não encontrei a resposta correcta, para satisfazer a minha dúvida. Como garantir para o usuário final.

JULIE HEDLUND: Que identificamos, Acho que deveríamos continuar avançando.Para que os participantes façam as perguntas no final da apresentação.

RUSS MUNDY: Aqui na parte de cima vamos ver se chama de navegador Bloodhound, é um derivado do *Firefox, Mozilla*. Tem capacidade total de DNSSEC, faz toda a verificação e esta acontecendo essa apropriação essa informação não está presente aqui. Se tratando de um navegador normal e literalmente quando vemos a barra de URL, cá em cima, você envia para o mesmo lugar, está pedindo a mesma informação, vocês podem ver. O navegador, não o DNSSEC recebe a informação de apropriação, mostrando Steve Crocker admite que o DNSSEC não resolverá de forma

mundial e nesse caso se propõem a fazer uma coisa muito óbvia, muito simples, que não é uma coisa real. Mas bom, estamos falando se apropriação. Muito bem. Passamos para uma *webpage*. Essa barra URL lá em cima, esta é uma imagem de quantas consultas são necessárias para um website comercial, Isto faz cinco anos e hoje é este o desenho. Para completar CNN.com, por exemplo, é necessário uma grande quantidade de consultas. O importante, mais uma vez, é que temos que ter os dados de zona correctos. E isso o DNS é isso, o mecanismo para fazer com que aconteça, mas os dados da zona, da região, são informação crucial que queremos que chegue no lugar certo no estado correcto. Aqui uma outra imagem, num outro gráfico que mostra simplesmente o que acontece. Não vou explicar o fluxo etc., estes slides aqui, estão na *website* também, se vocês quiserem podem revisar podem utilizar. È uma consulta padrão. Se Você colocar DNSSEC, dependendo de onde vocês estão na cadeia, neste processo vimos um ISP fazendo principalmente consultas recursivas, vimos a raiz *ponto.com*, *bigbank*. Há diferentes papéis em todo este processo, Mas seja onde for não importa o papel de cada um, etc.,. A sugestão geral vai ser que façam o mesmo tipo de coisas quando vão fazer DNSSEC. Então, o DNS crucial, importantíssimo qualquer que seja o papel que tenha o operador de gTLDs, ou se tem grande experiencia, uma muito importante experiencia, deverão trabalhar então nesse assunto, porque é muito importante. Importante treinar também as pessoas. Algumas terceirizam para outras empresas. Se vocês não conseguem, deverão decidir se vão terceirizar ou não. A não ser que vocês, por exemplo, escolham criar experiencias de DNSSEC na própria organização. Não importa o modo que vocês façam, por exemplo usuários de MAC que são cada vez mais frequentes, porque é uma plataforma muito simples

de construir. Existe o navegador Bloodhound, podem escolher como navegador por defeito. A zona da região do DNSSEC que oferece essa garantia. A última coisa que entra o DNS, pelas posições autorizadas para entrar nessa área nessa zona, é isso que o DNS nos diz, que essa informação que o DNS oferece, ao usuário final, etc. Nos Estados Unidos um fornecedor, um provedor de cabo muito importante está fazendo validação em muitos resolutórios para uns 18 milhões de clientes. Uma grande base de dados, estão fazendo a sua validação. Eu sou um cliente de Comcast, faço também os meus próprios resolutórios. Obrigado. Me esqueci de também Google. 8.8.8.8 e 8.8.4.4, fazem validação de DNSSEC, podem utilizar esta validação. Agora se vocês quiserem a ligação entre o computador e o validador vocês não vão ter nenhum problema. Vocês podem utilizar o DNSSEC, utilizando os seus validadores e do Google também. Então aqui vocês têm tudo o que devem fazer, depois que forem assinados os dados eles devem ser validados em lugar em seu computador, ou em seus servidores. Aqui escolhemos o servidor recursivo, também poderia ser no computador. Novamente, como princípio geral. Sim.OLAF. Você me queria dizer.

OLAF KOLKMAN: Então, em termos de números, Geoff Huston da *APNIC* fez uma pesquisa e estudou quantas pessoas que estavam protegidas pelo DNSSEC, e qual é o número dessa população. Então foi 8% dos usuários finais que estavam protegidos, que navegam na internet são protegidos por DNSSEC. Então dentro da infraestrutura do Google sobretudo, Mas é um número significativo de usuários da internet, protegidos de DNSSEC, ou seja, pensando do ponto de vista dos usuários.

RUSS MUNDY: Obrigado, eu me tinha esquecido deste número, Então onde Você estiverem, para fazerem essa operação do DNSSEC, devem ter o mesmo principio para ser o DNSSEC, e para garantir que tudo isso é um aspecto importante, com o seu provedor de *software* ou *hardware*, então vocês devem certificar. Se que podem pedir apoio do DNSSEC, porque durante muitos anos, houve muitos provedores perguntando, ode está a demanda? As pessoas devem solicita-las. Não está disponível agora é então hora de talvez substituir ou trocar de provedor. È este o conjunto de informação para as questões planejadas e estamos então abrindo o espaço para perguntas. Tenho uma pergunta que eu gostaria de fazer a todos vocês. Tenho estes slides, que eu apresentei aqui, para descrever como se fazem este tipo de ataque. Quando as pessoas fazem comentários se gostariam organizar uma rede sem fio para ver se seria valido. Alguém está de acordo, se voes querem fazer realmente na prática? Podemos fazer na próxima reunião da ICANN para mostrar que é real. Que não é apenas uma actuação. Podemos fazer isso com um computador de verdade. Se vocês têm algum outro comentário, podemos fazer isso, de verdade, com um computador de verdade. Tem uma pergunta ou comentário? Vocês podem fazer perguntas, por favor.

AUDIENCIA: A minha pergunta é como mais de um usuário final, e como uma bolsista de ICANN. Falando então de ameaças e da questão de roubo do DNS, eu gostaria de saber se isso é aplicado também para os aplicativos. Porque a maioria dos usuários, dos *websites*, utilizam aplicativos. A DNSSEC acrescenta mais uma camada, ou é mais arriscado utilizar os aplicativos.

RUSS MUNDY: JULIE por favor Você pode recuar alguns slides. Um pouco mais por favor. Mais por favor. Esse, ai está. Esse é o slide que eu queria. O navegador que vocês viram, faz de DNSSEC não é necessário ter aplicativos. Funciona com DNSSEC, poder ver o conteúdo. Vocês devem ter DNSSEC aplicativos, que suportem DNSSEC. Estão fazendo trabalhos para a interface para aplicativos já algum tempo que fazemos o trabalho, para que as aplicações possam ser padronizadas.

ROY ARENS: Eu entendi a sua pergunta de uma forma um pouco diferente. Os aplicativos em navegador, por exemplo. *Iphone* pode utilizar DNSSEC? È independente do aplicativo o DNSSEC. Se algum aplicativo utilizar DNS isso é o resolutor de ISP, todos os aplicativos iriam tirar proveito disso. Espero ter respondido á sua pergunta.

OLAF KOLKMAN: Eu gostaria de pensar de outra forma, quando utilizamos a internet, sempre que navegamos na internet, como tudo o que fazemos na vida, utilizamos DNS, quer seja agenda, enviar um *email*, ver noticias, enviar uma mensagem, fazer inclusive uma ligação telefónica, via *internet*. Se utiliza DNS como recurso para poder chegar a algum lugar. E todos esses, que eu acabo de mencionar, têm valor. Também há um factor para poder atacar nesses pontos. Se ligamos DNSSEC introduzimos uma camada adicional para todos os aplicativos, que não necessariamente utilizamos. No backend quando utilizam é a mesma resposta dita de

outra maneira.

JULIE HEDLUND: Temos microfone aí atrás. È uma pergunta remota, sim é possível faze-la. Não deu para escutar muito bem. Temos uma pergunta do Ade Bumbekimbo, não sei, se pronunciei bem.

ADE BUMBEKIMBO: A pergunta é a seguinte. Como podemos desdobrar um ISP, que temos que fazer para ter a garantia que será usado, funcionando num ccTLD?

ROY ARENS: Na verdade eu trabalho num CCTLD no Reino Unido. Passamos já por essa etapa. Esta é para uma pessoa que está fazendo um CHAT. Se respondesse levaria muito tempo. Mas não há nada de novo aqui. Há muitos países que já implementaram o DNSSEC. À muita informação a respeito disso. No DNSSEC-2.org que vocês podem encontrar, que vocês têm que assinar para poder chegar até ao servidor raiz, mediante muitos testes. Quando assinamos alguma coisa, significa, basicamente, que fornecemos uma espécie de autenticação. Digamos que não ciência quântica. Á 10 ano talvez fosse difícil fazer isso, mas hoje em dia á muitas ferramentas e documentos. Russ os seus slides, com muitos *links,* vocês podem encontrar a informação ali disponibilizada. Você gostaria de acrescentar algo Russ.

RUSS MUNDY: Sim, gostaria de destacar parte das estatísticas que fazemos são assinadas na zona raiz dos TLDs, e continua crescendo, esse índice continua aumentando. Antes, como eu lhes disse, a maneira como fazem o DNS, se vocês forem provedores de TLD ou proprietário e se tiverem um parceiro, que por exemplo, possa ser um operador, talvez possa ter um parceiro de TLD, que já seja capaz de fazer e implementar DNSSEC. Talvez não seja mais complexo do que falar com os seus parceiros, se eles já utilizam DNSSEC e activa-lo para a sua zona. Como disse Roy, começando a partir de zero fazendo a verificação e os testes para garantir que todo possa funcionar, até, e torná-lo operativo ou funcionando. Vamos ver. Adiante, por favor. A sua pergunta.

AUDIENCIA: Você já utilizaram DNSSEC para os seus emails, porque quarenta por cento dos *emails* enviados, no mundo inteiro, e *spam*. Eu trabalho para varias companhias. Há milhares de spam nos correios eletrónicos. Nos *emails*. è o maior problema é que muitas vezes os emails. Válidos ficam atrelados no *spam*. Como vocês abordam esta questão.

RUSS MUNDY: Roy tinha mencionado isso anteriormente. Todos os aplicativos que estão a ser tocados por uma máquina, podem tirar proveito. Já foram feitas algumas implantações, especificamente para alguns SMTP e IMAP, para ver se utiliza DNSSEC. Mas a maior parte das actividades realizadas é utilizar a tecnologia juntamente com o DNSSEC para ajudar a reforçar os SMTPs.

ROY ARENS: Há protocolos que já foram implantados e padronizados que podem utilizar coisas como por exemplo o DKIM, DMARC e outros mecanismos de segurança. No entanto, e eu gosto desta frase, as pessoas roubam bancos também tem isto e também utilizam este tipo de mecanismos de segurança. E o DNSSEC também, acaba por ser utilizado. As pessoas que enviam *spam*, o lixo eletrónico, também utilizam o DNSSEC. Afinal das contas terminamos não abordando o problema.

PAUL DONOHOE: Ola sou o PAUL. Sou um dos patrocinadores de *ponto.dob* estamos participando de algumas conferências de DNSSEC. Obrigado pela sua explicação tão simples de um assunto tão complexo. Tenho uma serie de questões e gostaria de fazer algumas perguntas. *ponto.post* está baseado totalmente num DNSSEC e assinado pelo DNSSEC. È um desafio para a comunidade particularmente como TLDs. Estamos trabalhando muito em regiões com nome e domínio. Então, porque é uma adopção lenta em questões de infraestrutura, em regiões como Africa. È um dos desafios que estamos enfrentando. E uma das perguntas que eu gostaria de fazer então. Como podemos ter uma melhoria na infraestrutura nessas reuniões e o que podemos fazer então para fomentar a adopção. E a outra pergunta está relacionado como nós, como usuários, sentados diante do nosso computador podemos nos sentir mais confortáveis com um *website* e como eu posso saber que um website é seguro. Essa é uma das perguntas que são feitas por muitos usuários, e nós sempre dizemos que utilizam o DNSSEC, que tudo está assinado, que isto é seguro. E como podemos nós transmitir

essa segurança aos usuários? Para que eles possam sentir que isso é seguro.

ROY ARENS: Vou procurar responder essas perguntas. Bom a primeira pergunta então., Eu vou ser um pouco mais genérico. A pergunta seria como a adopção do DNSSEC, no nível dos domínios de segundo nível ou no nível dos domínios de primeiro nível.

PAUL DONOHOE: Isto tem a ver com os nomes e com os proprietários dos domínios que estão preocupados, por isso eu tenho a infraestrutura já implementada dentro do meu operador de registos. Mas como fazemos para que essas capacidades possam ser implementadas nas nossas estruturas?

RUSS MUNDY: O senhor está perguntando sobre o nome, sobre *ponto.post*? O operador de registo está pronto? Seja quem for que operar o DNSSEC, poder ser um Pais, por exemplo, que no caso de "post" seria comum, ou outra entidade, um banco, seja a instituição que for. Se não houver um mandato de política realizado, as pessoas não gostam muito disso, porque é difícil. Como o Roy disse anteriormente há muitas ferramentas disponíveis grátis e às vezes é uma questão de saber onde elas estão. E se as pessoas, no seguinte nível imediato, pode realizar

Isso, no entanto há forma em que o DNS funciona pode, talvez possa, variar porque pode então passar para outro operador. Então temos que

ver se este operador pode implementar o DNSSEC. Então outra coisa seria, encaminhar o negócio para outro lugar, porque há muitos operadores e nomes, que estão procurando, operar. Porque eles já possuem o DNSSEC implementado, muitas vezes isto é uma questão de ajudá-los a evoluir, em vez de ficarem estagnados.

ROY ARENS: Havia uma segunda pergunta, certo? Talvez na Suécia e nos países baixos, na Holanda, são pioneiros na adopção do DNSSEC. Parte do sucesso disso, para esta questão, tem a ver com o marketing. E um pouco também com os descontos oferecidos, quando se registam um domínio DNSSEC.Em relação a essa segunda pergunta tinha a ver com usuários finais. E se usuário final beneficia do DNSSEC. Como usuário pode ver se o website, que ele está consultando, é seguro. Actualmente não temos implementado em produção. Em andamento, Os provedores muitas vezes operam sobre *ponto.x* o sobre *windows* e então basicamente se isso foi implantado, ou com um nome, o um nome de domínio, ou um domínio de alto nível. Eu hoje de tarde escutei sobre um projecto que está sendo realizado com um domínio de alto nível para poder estabelecer um padrão para esse tipo de dinâmica, para os usuários. Não se vocês poderem participar nisso. Agora está falando outro orador, Sim eu interagi muito empolgado.

OLAF KOLKMAN: Eu sou Olaf Kolkman. E trabalhamos como por exemplo NLnet Labs na comunidade durante uma década. Procurando implementar o DNS e do DNSSEC, quanto ao que acabou de mencionar agora estamos

interessados em ver como fazer chegar o DNSSEC aos utilizadores e também aos aplicativos. A pergunta que o senhor fez, basicamente, tem a ver com uma interface com os usuários, que não é a nossa especialidade, mas tem a ver com os aplicativos utilizados, que utilizam DNSSEC. Em muitos casos nas interfaces e nos aplicativos não oferecem esta possibilidade. Então estamos trabalhando com *IETF* com um grupo de pessoas que estão procurando desenvolver aplicativos para pode proporcionar essa capacidade para os programadores. Mas voltando um pouco á outra questão e talvez com um outro enfoque, em relação á sua pergunta. Às vezes acreditasse que o que pode ser feito para criar inovações no mundo inteiro ocorre com o IPV6 como podemos estrutura central da internet. Quando falamos em inovações, no geral há muito trabalho feito pelos profissionais de marketing e basicamente se considera quais as questões que as pessoas gostariam de adoptar. Por exemplo as vantagens relativas á complexidade e simplicidade que possa ter uma inovação uma incompatibilidade a capacidade de uso, etc. A inovação que o senhor, daquilo que acabamos de falar, o usuário vê que é uma vantagem utilizando isso. O DNSSEC é a tecnologia que ainda não foi utilizada completamente. A ver questões que são vantagens, mas que são difíceis de serem reconhecidas e também há vantagens a longo prazo. Essas são as vantagens que estamos comentando aqui. A segurança a longo prazo para estrutura ou infraestrutura global. Não é uma coisa para, unicamente para nós., somente quando falamos sobre tudo do lado dos provedores. Mas o que queremos é proteger a internet e inovar. Quando pensamos de forma mais colectiva, e talvez o senhor compartilhe essa ideia comigo, temos que garantir então que há complexidade e a compatibilidade possa reduzir as barreiras existentes., Por isso temos software livre, por

isso temos ferramentas de design que são disponibilizadas de código aberto para este tipo de projectos. E outra questão também. É criar incentivos. Por exemplo, na Holanda havia um subsídio onde se assinássemos o nome de domínio, a tarifa era menor. Era uma pequena percentagem para as companhias de hospedagem, que tem milhares de domínios, essa era uma proposta bastante interessante. Então com o registo no nível de registo são questões que podem ser implementadas. Garantindo também que a comunidade de usuários tenha acesso simples. Possam aceder facilmente a esse tipo de ferramentas e que possam receber também incentivos financeiros. Isto é então para o bem pública. Espero que esta possa responder à sua pergunta a partir de uma perpectiva não tão tecnológica.

PAUL DONOHOE: Estou de acordo. E também com o DNS as vezes garantir uma estrutura de DNSSEC é muitas vezes implica custos, e as vezes o usuário final é quem termina decidindo o que vai utilizar. Então acredito que deveríamos seguir debatendo essa questão. Sim mas temos que colocar o foque nisso.

RUSS MUNDY: Em outras sessões também, por exemplo na quarta-feira, o dia inteiro, vamos aprofundar essas questões. Um dos temas importantes que eu acredito que vai nos ajudar, como chegar até ao usuário é a introdução de certas tecnologias. E é claro na quarta-feira vamos tratar este tema mais profundamente, Mas isto é uma coisa que pode ser mais motivadora uma maneira de fazer com que a informação possa chegar

até ao usuário, numa forma mais simples. Mais alguma pergunta? Lá atrás, há um *Chat room*.

CARLOS WATSON: Qual é o desafio do ISP para promover o DNSSEC no resolutor? Qual é o problema então para a adopção do o ISP a muitos DNS, muito obrigado.

RUSS MUNDY: Pode repetir a pergunta?

CARLOS WATSON: Qual é o desafio para o ISP para promover a adopção do DNSSEC num resolutor?

RUSS MUNDY: È uma questão que devemos resolver. È uma questão que deverá ser resolvida. Se entendi bem a pergunta, acho que a pessoa está perguntando o que é necessário para que os operadores de resolutores em todo o mundo implementem e comecem a utilizar DNSSEC. Acha que se aproxima da pergunta? Tem a ver com isso? Uma das coisas importantes que realmente é um grande factor é que é uma demanda em toda a sala todo o mundo podia aqui voltar e ver o que está fazendo o ISP. Seja no trabalho, em casa o ISP do seu lar está fazendo DNSSEC. 8% é uma opção. È boa, mas isto ainda deixa 92% fora. Este é um dos grandes motores que existe, que as pessoas proponham o assunto de modo a que seja compreendido a demanda é o melhor. Exigir, falando

sobre em torno competitivo, os ISP são na maioria, Esse ambientes em alguns Países, o governo é que tem o controlo. Nesses casos vocês podem trabalhar com os governos que participam no controlo desse aspecto para promover precisamente a adopção de DNSSEC.

WARREN KUMARI: O que fizeram algumas pessoas como o Comcast, por exemplo, é que existe um pequeno custo para habilitar de DNSSEC no resolutor desse evento, Há um custo adicional que é um pouco mais, nem tanto. O que vocês podem fazer, que uma vez, que habilitaram, podem dizer aos usuários, que o grande trabalho que estão fazendo de ajudar com a segurança, pode utilizar como uma ferramenta de marketing ou de vendas para dizer aos usuários que vocês estão ocupados com isso, que vocês mantem estas trocas entre os usuários sendo seguras. Então esse seria um diferenciador importante. Se eu escolhesse um ISP preferiria um que se responsabilizasse pela segurança. Eu quero que as transações sempre sejam seguras, das que não cuidam da segurança. Utilizar isso como uma ferramenta de vendas. Vai ser uma coisa muito boa. E também alguns ISPs na região que eu já digo. Vocês não estão fazendo e acontece alguma coisa com algum usuário, ele pergunta, e com toda a razão "porque não fizeram todo o possível para manter a segurança, porque não, porque estão fazendo agora, vocês talvez estejam se arriscando de forma bastante importante na área judicial".

JOYCE: Eu simplesmente queria conferir que eu entendi, ver se vocês podem esclarecer. Quando DNSSEC os actores se a zona área raiz é assinada e o

servidor DNS a companhia que administra o servidor de DNS também assina, todos os domínios são assinados. Então quem mais deveria fazer o trabalho? Pelo o que eu entendo os ISP, por exemplo no meu caso, eu utilizo uma companhia de cabo para internet. Eles também são responsáveis, eles também devem fazer DNSSEC. Eu pensei que os servidores de nome, deveriam, parece então que é muitos actores que devem fazer o trabalho, o seu trabalho.

RUSS MUNDY: Quero esclarecer isso para a JOYCE. O que vimos antes na peça de teatro é que na primeira parte era feito sem DNSSEC, consulta e respostas sem DNSSEC. O senhor ISP era quem ia e fazia todas as perguntas para os diferentes servidores de nomes. Depois o doutor malvado, ia e roubava a informação. Mas poderia ter feito a qualquer momento, Mas quando tudo fica assinado, se não temos um resolutor de servidor de nomes validando com o ISP, no nosso caso, o usuário nem sequer saberia se o dados foram assinados. E portanto também não saberia quem tem a informação em papel. Realmente importante para o resolutor ou para o operador de ISP ou para o usuário final, justamente fazer a validação da consulta, obter os dados que sejam assinados, mas menos a validação é muito importante, mas não obtemos a vantagem do DNS. O DNS se obtém a qualquer momento. Vocês entendem a diferença?

JOYCE: Mas quando foi assinado o domínio, o DNS você falou num aplicativo *API* o programa para o qual vocês trabalham também deveria estar

assinado?

RUSS MUNDY: Não os aplicativos não devem saber nada, em absoluto de DNSSEC. Desde que, os resolutores de DNS, estejam a fazer a validação do DNSSEXC. Esteja o resolutor na máquina do usuário ou no ISP. Os aplicativos não, se souberem melhor, mas não deveriam, não é uma exigência. Muito bem. Mais perguntas?

CRAIG NESTY: Sou Craig Nesty de Dominica. Vi na representação, no final da peça que vocês representaram, no último passo, quando acontecia a apropriação, o sequestro, o apropriador não corre DNSSEC o resolutor praticamente atrapou, o que aconteceu ao servidor hospede que não corre DNSSEC, é compatível com outras versões anteriores, recusaria ou não esse *website*.

RUSS MUNDY: O desenho DNSSEC se adapta se ajusta a coisas que não estão assinadas, também com coisas que estão assinadas. Quando levamos as respostas para as consultas de DNS temos às vezes um ponto na árvore, e que não há assinaturas de DNS. Isso significa, isso pode ser identificado dentro do protocolo de DNSSEC.O modo em como funciona a resolução reconhece como não assinado, e opera então. Não recusa e não supõem que esteja assinado.

AGOSTINHO SACRAMENTO: Sou desenvolvedor de NIC na Argentina. Eu poderia fazer um aplicativo para ditar a assinatura para cada passo da cadeia. Um aplicativo, por exemplo, a partir de um telefone móvel, um celular. Eu quero que o programa me diga que a conexão é DNSSEC, poderia detecta-la?

RUSS MUNDY: Existem implementações que correm que bolam o celular em telefones móvel, *Android* e alguns outros que funcionam com sistema operacional, o telefone móvel. É bem possível esses serem assinados. Então a questão é examinar qual a base do código, qual o aplicativo que Você quer utilizar. Então começar a iniciar dentro das especificações, escrever o código é muito possível. E talvez poderemos fazer, faça, se precisar de ajuda, esta é uma comunidade incrivelmente útil. Há muito trafico em laboratórios da *internet*, há muitas perguntas sobre o que se faz, sobre a ajuda recebida pelas coisas que fazem, claro por favor continuem, é possível, talvez não seja fácil mas se Você conhecer a plataforma e o *software* faça, faça.

JULIE HEDLUND: Russ, já estamos, terminou o nosso tempo. Só uma pergunta?

SPEAKER: Julie. Uma pessoa lá atrás da coluna que está levantando a mão para fazer a pergunta. A pergunta pro favor?

AUDIENCIA: A minha pergunta é. Há alguma relação entre DNSSEC e SSL. *Secure Socket Layer?*

RUSS MUNDY: São dois protocolos independentes, são complementares, poderíamos usar um. Um funciona bem com outro, obteríamos maior segurança, se os dois forem utilizados. Mas são independentes, Eles podem ser operados ao mesmo tempo, na mesma máquina e talvez algumas destas pessoas aqui estão fazendo nos meus *laptops*, eu não faço mas é muito bom. Seguranças múltiplas em diferentes camadas de protocolo é muito útil é muito bom. Respondi á pergunta?

AUDIENCIA: Muito bem. Obrigado.

RUSS MUNDY: Acho que é tudo, é isso. Muito Obrigado, foi uma sessão muito boa, muito interessante. Se vocês estiverem na próxima reunião nos vemos.

JULIE HEDLUND: Obrigado.