# DNSSEC

Nomes: Flávio,Ienne,Rosane

RESUMO

O objetivo do trabalho é dar uma pequena introdução ao uso de DNSSEC (Domain ame System Security Extensions) e ajudar a entender como a sua utilização pode ajudar a atenuar um dos diversos problemas de segurança que enfrentam os administradores de redes de grandes, médias e pequenas organizações. Como todo serviço de rede é suscetível a falha, a segurança com que as informações que trafegam pelos canais de comunicação entre as empresas e os clientes exigem que cada vez mais procedimentos sejam adotados, a fim de garantir a autenticidade das informações desde o seu início até o termino do processo.

O que DNSSEC propõem é uma maior segurança no sistema de resolução de nomes, reduzindo o risco da manipulação dos dados e domínios forjados. Baseado na tecnologia de criptografia que emprega assinatura, o DNSSEC utiliza um sistema de chaves assimétricas em sua tecnologia de trabalho.

A sua utilização vem crescendo vertiginosamente no último ano e isso leva a acreditar que poderá até mesmo ser a referência utilizada para resolução de nomes, visto que, no estágio atual, a certificação pelo nome usando o DNS (Domain Name System) é altamente insegura.

INTRODUÇÃO

Não é surpresa que,com a invenção da internet,com todos seus endereços numéricos de Protocolos de interne ,os humanos precisassem de um meio de traduzir esses números em nomes mais compreensíveis.O Sistema de Nomes de Domínios DNS foi criado em 1983 para permitir que nós,humanos,fôssemos capazes de identificar pelo nome todos os computadores,serviços e recursos conectados à internet.O DNS traduz nomes legíveis para os humanos em informações binárias exclusivas para os dispositivos,para que os usuários de internet sejam capazes de encontrar as máquinas que quiserem.Pense nele como a lista telefônica da internet.

Agora,o que aconteceria se alguém trocasse o nome da sua empresa,colocando no lugar o nome dele?A lista telefônica relacionaria "O HACKER",um impostor que receberia todas as ligações destinadas a você e controlaria seu número.Ou,que tal se alguém excluísse todas as referências a você e ninguém mais pudesse encontrá-lo?Isso com certeza afetaria seus negócios. E se a mesma situação acontecesse com o nome do domínio ligado ao seu site público? E se fosse um site de comércio eletrônico!

Ou seus clientes não poderiam encontrá-lo de forma alguma ou eles seriam redirecionados a outro site que poderia parecer exatamente igual ao seu,mas que na verdade era o site do “hacker”.Ele ficaria feliz em tomar todos os seus pedidos e pagamentos,deixando você sem receita,paralisado ou com todas as outras miríades de problemas que surgem quando uma propriedade na Web é sequestrada.

Segurança não foi um item incluído no planejamento original do DNS,já que na época o principal problema era a capacidade de se expandir,e não o comportamento mal-intencionado.Muitos acreditam que proteger o DNS seria de imensa ajuda para proteger a Internet como um todo.A Extensão de Segurança do Sistema de Nomes de Domínios (DNSSEC) pretende acrescentar segurança ao DNS sem perder a compatibilidade com o sistema antigo para poder crescer junto com a Internet.Em essência,o DNSSEC adiciona uma assinatura digital para garantir a autenticidade de certos tipos de transação com o DNS e,dessa forma,garantir a integridade da informação. O DNS fez um excelente trabalho desde seus primórdios,porém,como

ocorre com tudo mais na Internet,pessoas mal-intencionadas descobriram como explorar o protocolo.

A autenticação é o processo de identificar com quem está se trocando informações sigilosas, ou seja, é o processo de confirmação se o destinatário é realmente quem você desejou contatar. Na nossa vida real podemos identificar outras pessoas através de suas feições, características e demais semelhanças que são percebidas aos olhos, e as comprovações são feitas através de assinaturas em contratos ou qualquer meio que caracterize um compromisso firmado, com símbolos em alto relevo e através de outras formas de reconhecimento.

Geralmente as falsificações são detectadas por especialistas em caligrafia, papel e tinta. Infelizmente estas opções não estão disponíveis no mundo digital, por isso está muito claro que são necessárias outras soluções.Basicamente as redes de computadores não são seguras. Existem muitas soluções para se implementar segurança em uma rede.

Pode-se escolher dentre varias opções; ações implementadas  desde ao nível da camada física até ao nível da camada de transporte, pois existem possibilidades variadas de tecnologias para segurança. Uma das soluções mais adotadas visando manter o sigilo das informações enviadas em uma rede de dados consiste no uso da criptografia, ou seja, as informações são embaralhadas de tal maneira que só os computadores autorizados consigam resgatar a informação na sua forma original.

O DNSSEC é um mecanismo proposto para tornar o protocolo DNS seguro. É composto de uma série de extensões ao DNS, a qual fornece autenticação e integridade fim a fim e foi projetado para proteger a internet de certos tipos de ataques, como DNS spoofing.

Para que se possa visitar uma pagina Web ou quando pretende enviar uma mensagem eletrônica, o navegador ou o cliente de e-mail precisa saber em qual servidor essa pagina está hospedada e o e-mail esta armazenado para poder responder à sua

solicitação. Esta informação sobre a localização dos servidores fica armazenada em servidores chamados DNS (Sistema de Nomes de Domínios).

O servidor DNS traduz nomes para os endereços IP (Internet Protocol) e endereços IP para nomes respectivos, e permitindo a localização de hosts em um domínio determinado. Para cada domínio existe um registro no DNS que define qual o endereço IP do servidor de hospedagem e o IP do servidor de e-mail que responderão por este domínio.É denominado resolução de nome ou resolução de domínio o processo que permite a descoberta do servidor que responde por um determinado domínio.

Todo o processo de resolução de nomes que ocorre para que uma mensagem seja enviada ou uma página Web seja acessada não é transparente para o usuário.Ele apenas sabe que sua solicitação foi atendida. Por medida de segurança, um domínio pode definir vários servidores DNS, sendo sempre o servidor DNS primário o primeiro sistema a ser consultado para tentativa de resolução de nome e caso o mesmo venha a falhar ou não estar disponível entra em ação o próximo servidor de consulta que é o servidor DNS secundário uma espécie de cópia de segurança do servidor DNS primário e continua assim sucessivamente até que se obtenham a resposta solicitada.

O protocolo DNS utiliza o protocolo de transporte UDP (User Datagram Protocol) para as tradicionais requisições devido ao baixo overhead e melhor desempenho. E utiliza o protocolo TCP (Transmission Control Protocol) para a funcionalidade de transferência das zonas.A estrutura do banco de dados DNS é um sistema de gerenciamento de nomes distribuído e hierárquico, ao invés de um banco de dados central e único, a resolução ocorre consultando diversos servidores DNS e sua resolução é hierárquica.

A estrutura hierárquica é equivale a uma árvore invertida, existindo um servidor principal que aponta para um secundário que aponta para um terceiro e assim sucessivamente. Em virtude do banco de dados de DNS ser distribuído, seu tamanho é ilimitado e o desempenho não degrada tanto quando se adiciona mais servidores nele.O servidor DNS que está no topo da internet é o servidor raiz.

O servidor raiz da internet possui uma tabela que indica qual DNS será responsável pela resolução dos domínios para cada extensão de domínio TLD (Top

Level Domain) diferente. A tabela em si é muito pequena, possui apenas uma entrada para cada TLD existente. Os TLDs são de dois tipos: gTLDs (Generic Top Level Domains -domínios genéricos usados no mundo todo) e ccTLDs (Country Code Top Level Domains-extensões de domínios administrados pelos países).

Existem 13 servidores DNS raiz no mundo todo, que são conhecidos como root servers, destes, dez estão localizados nos Estados Unidos da América, um na Ásia e dois na Europa. Para aumentar a base instalada destes servidores, foram criadas réplicas localizadas por todo o mundo, inclusive no Brasil. Ficou convencionado que cada servidor seria chamado por uma letra do alfabeto (Server A, Server B e assim por diante) que podem ser replicados em diversos lugares do mundo para que o tempo de uma consulta tenha menor latência em relação à consulta ao próprio servidor.

O DNS fez um excelente trabalho desde seus primórdios,porém,como ocorre com tudo mais na Internet,pessoas mal-intencionadas descobriram como explorar o protocolo. Um dos modos é chamado de envenenamento do cache do DNS.Quando você digita uma URL no navegador,um solucionador de DNS verifica na Internet o nome/número correto da transação e localização.Geralmente, o DNS aceitará a primeira resposta ou responderá sem perguntar e enviará você ao site.Ele também guardará essa informação por um período até que ela expire,assim da próxima vez que o nome/número for requisitado,o site é fornecido imediatamente.

O DNS não precisa consultar a Internet novamente e usa o endereço até ele expirar.Como os usuários supõem que estão obtendo a informação correta,a situação pode ficar crítica quando um sistema malicioso responde à primeira consulta do DNS com uma informação falsa,modificada, e assim tem-se o envenenamento do DNS.Os servidores de DNS primeiro enviam o usuário ao link errado,mas também guardam a informação falsa até ela expirar.

Não é apenas um computador que é enviado ao lugar errado; se o servidor malicioso estiver respondendo ao serviço de um provedor,milhares de usuários podem ser enviados ao sistema desonesto.Isso pode durar horas ou dias,dependendo de quanto tempo o servidor armazena a informação,e todos os outros servidores de DNS que propagam a informação também são afetados.O perigo iminente oferecido por um site

desonesto inclui o fornecimento de um malware,a perpetração de fraudes e o roubo de informações pessoais ou sigilosas.

O DNSSEC é uma série de extensões ao protocolo do DNS,definidos nas Requisições de Comentários (RFCs) 4033,4034 e 4035,que asseguram a integridade dos dados retornados pelas consultas de nome de domínio ao incorporar uma cadeia de confiança na hierarquia de DNS.A cadeia é construída usando-se uma infraestrutura de chave pública (PKI),com cada elo na cadeia consistindo em um par de chaves pública e privada.O DNSSEC não criptografa nem fornece sigilo aos dados,mas os autentica. O DNSSEC faz o seguinte: Autenticação da origem dos dados do DNS:Os solucionadores podem verificar se o dado se originou em um serviço confiável.Integridade dos dados:Os solucionadores podem verificar se a resposta não foi adulterada durante o envio. Negação de existência autenticada:Quando não houver resposta à consulta,os servidores confiáveis podem fornecer provas de que não há dados.

Implementar um DNSSEC implica autenticar zonas com criptografia pública/privada e devolver as respostas do DNS com assinaturas.Um cliente confia que essas assinaturas são baseadas em uma cadeia de confiança estabelecida além das fronteiras administrativas,de zonas pai para zonas filhas,usando uma nova DNSKEY e registros de recursos com autenticador de delegação (DS).Uma implementação de DNSSEC precisa gerenciar as chaves criptográficas:geração de múltiplas chaves, autenticação de zoneamento,troca de chave,revisão e temporização de chaves e recuperação de chaves comprometidas.

## CONCLUSÃO

Concluímos que o objetivo do DNSSEC é permitir que os servidores de DNS consigam autenticar as respostas das resoluções de nomes.Se um invasor conseguir falsificar um endereço IP para o site verdadeiro ,o servidor de DNS,usando o DNSSEC,poderá verificar que aquela resposta não é a correta e assim saberá que deve descartá-la e tentar descobrir o real endereço do site novamente,até obter a resposta certa.E concluímos que com associado a utilização de outros protocolos e soluções de segurança o DNSSEC será de grande contribuição para que seja reduzido o risco de um cliente e entre outros serem enganados por um falsário que tenta se passar pelo sistema de um banco,com intuito de capturar informações privilegiadas.

## REFERÊNCIAS


www.ietf.org

ftp.registro.br/pub/doc/tutorial-dnssec

www.mp.br/newsgen

http://www.sacsis.ufv.br

http://webinsider.uol.com.br/2007/10/13/o-que-e-dns-e-dnssec-bem-explicadinho/