**Resumo do LEE**

O padrão de Autenticação de Entidades Nomeadas (DANE) com base em DNS permite que clientes e servidores estabeleçam uma conexão TLS sem depender de terceiros confiáveis, como CAs, publicando registros de Autenticação de Segurança de Camada de Transporte (TLSA). O DANE usa as Extensões de Segurança do Sistema de Nome de Domínio (DNSSEC) PKI para obter integridade e autenticidade. No entanto, o DANE só pode funcionar corretamente se cada um dos principais em sua PKI desempenhar adequadamente sua função: por meio de seus servidores DNSSEC compatíveis, os servidores DANE (por exemplo, servidores SMTP) devem publicar seus registros TLSA, que são consistentes com seus certificados. Da mesma forma, os clientes DANE (por exemplo, clientes SMTP) devem verificar os registros TLSA dos servidores DANE, que também são usados para validar os certificados buscados.

O DANE está ganhando popularidade rapidamente no ecossistema de e-mail, para ajudar a melhorar a segurança do transporte entre os servidores de e-mail. No entanto, seus benefícios de segurança dependem da implantação correta do DANE. Neste artigo, realizamos um estudo de medição em larga escala, longitudinal e abrangente sobre o quão bem o padrão DANE e seus protocolos relevantes são implantados e gerenciados. Coletamos dados para todos os domínios de segundo nível nos TLDs .com, .net, .org, .nl e .se durante um período de 24 meses para analisar a implantação e o gerenciamento do lado do servidor. Para analisar a implantação e o gerenciamento do lado do cliente, investigamos 29 provedores de serviços de e-mail populares, quatro MTA populares e dez programas de software DNS.

Nosso estudo revela má gestão generalizada no ecossistema DANE. Por exemplo, descobrimos que 36% dos registros TLSA não podem ser validados devido a registros DNSSEC ausentes ou incorretos, e 14,17% deles são inconsistentes com seus certificados. Também descobrimos que apenas quatro provedores de serviço de e-mail oferecem suporte ao DANE para e-mails enviados e recebidos, mas dois deles têm desvantagens de não verificar o uso do certificado nos registros TLSA. Por outro lado, os administradores de servidores de e-mail podem aproveitar os programas de MTA e DNS de código aberto para dar suporte ao DANE corretamente.

**Conclusão do LEE**

Este artigo apresenta um estudo longitudinal e abrangente do ecossistema DANE em SMTP - abrangendo 178 milhões de domínios de segundo nível e 29 provedores de serviço de e-mail populares para entender as implicações de segurança de como o DANE é (mal) gerenciado. Descobrimos que (1) a implantação do DANE é escassa, mas está aumentando, (2) mais de um terço de todos os registros TLSA não podem ser validados devido a registros DNSSEC ausentes ou incorretos e (3) 14% dos certificados são inconsistentes com seus TLSA registros. No lado do cliente SMTP, medimos 29 provedores de serviços de e-mail populares para entender como eles oferecem suporte ao DANE; descobrimos que apenas quatro deles suportam DANE para e-mails enviados e recebidos, e um provedor de serviços de e-mail o faz apenas para e-mails recebidos. Também testamos quatro programas de software MTA e dez DNS e descobrimos que dois programas MTA e sete programas DNS suportam o DANE corretamente, o que implica que os administradores dispostos a implantar o DANE não encontrariam nenhum desafio operacional.

**Resumo do Sandelin**

A autenticação baseada em domínio de entidades nomeadas (DANE) é um padrão da Internet Engineering Task Force (IETF) lançado em 2012 com o objetivo de complementar ou, em alguns casos, substituir o modelo atual de infraestrutura de chave pública (PKI). O modelo PKI atual usa certificados Transport Layer Security (TLS) emitidos por Autoridades de Certificação (CA) vinculando nomes de domínio à chave pública. Essas CAs atuam como âncoras de confiança durante o processo de validação do certificado. Os navegadores da web e outros aplicativos com suporte TLS têm grandes listas de chaves públicas de CA confiáveis. Se uma dessas CAs confiáveis for comprometida, todo o sistema ficará comprometido. O DANE usa o Sistema de Nome de Domínio (DNS) para publicar informações de certificado TLS e criar associações de certificado para nomes de domínio. DANE conta com DNS Security Extensions (DNSSEC) para autenticação e integridade da mensagem. Usando a raiz do DNS como uma única âncora de confiança, em vez das muitas âncoras de confiança da CA, a superfície de ataque é drasticamente reduzida.

Em 2012, o IETF publicou o RFC6698 que continha as especificações para um novo protocolo: Autenticação baseada em domínio de entidades nomeadas (DANE), que permite que as informações do certificado TLS sejam publicadas usando a infraestrutura DNS.

Por ser um protocolo relativamente novo, há uma quantidade limitada de estudos sobre os vários aspectos do DANE, como segurança, desempenho e níveis de implementação.

Este estudo tem como objetivo estabelecer o nível de implementação atual entre os domínios de segundo nível no domínio sueco de primeiro nível .se, realizando uma pesquisa dos servidores DNS autorizados para esses domínios para registros de recursos DANE TLSA.

**Conclusão do Sandelin**

Este estudo teve como objetivo estabelecer o nível de implantação do DANE TLSA entre os SLDs dentro do TLD .se; esse objetivo foi alcançado juntamente com a resposta bem-sucedida às questões de pesquisa.

O número de domínios assinados DNSSEC que foram validados com sucesso era grande. Em aproximadamente 676k domínios, este é um grande grupo de domínios que poderia implantar o DANE TLSA para seus serviços fornecidos para aumentar a segurança para os usuários desses serviços. Isso fornece uma resposta para a pergunta número um da pesquisa.

O estudo mostra que em 20-21 de abril de 2017, o nível de implantação de DANE TLSA entre SLDs suecos é extremamente baixo, com apenas 79 (~ 0,01%) das zonas assinadas DNSSEC disponíveis implementando DANE TLSA RRs em DNS. Isso fornece uma resposta para a pergunta número dois da pesquisa.

O estudo mostra que o serviço mais comum implantado em conjunto com DANE TLSA são os serviços que usam HTTPS na porta 443. Embora o número de domínios que implementam DANE TLSA para HTTPS ainda seja muito pequeno, apenas 59 domínios têm TLSA RRs em DNS para HTTPS. É possível que a atual falta de suporte nativo para DANE TLSA em navegadores da web esteja mantendo os níveis de implantação baixos. Isso fornece uma resposta para a pergunta número três da pesquisa.

O uso de certificado três é usado por 66% dos domínios que implantam DANE TLSA RRs e o uso dois outros 31% e, juntos, esses casos são usados por 97% dos domínios que implantam DANE TLSA RRs. Essa descoberta é interessante, pois ambos os casos de uso não usam o modelo tradicional de PKI da web pública ou a validação de PKIX para validar os certificados. Isso indica uma relutância em confiar em CAs de terceiros para assinar certificados. Isso fornece uma resposta para a pergunta número quatro da pesquisa.

**Resumo do Van Dongen**

A segurança do e-mail não foi levada em consideração durante o projeto original dos protocolos de e-mail. Portanto, diferentes técnicas surgiram para proteger a comunicação por email e validar emails. Muitos governos definiram diretrizes que exigem ou recomendam fortemente a adoção dessas técnicas para melhorar a segurança do e-mail. Esta pesquisa investiga quais e quantas dessas técnicas foram adotadas por organizações na Holanda. Uma lista de organizações holandesas com mais de 10 funcionários foi obtida de dois sites (no total 46.650 organizações exclusivas) que foi usada como entrada para o experimento. A organização holandesa chamada Standardization Forum definiu uma lista de técnicas de segurança de e-mail obrigatórias. Uma ferramenta da 'internet.nl' foi usada para verificar se essas técnicas de segurança de e-mail foram ou não adotadas por organizações holandesas. Encontramos uma relação entre os tipos de setores. O setor de 'serviço público' tem a pontuação mais alta. Assumimos que a pontuação mais alta está relacionada a políticas obrigatórias para organizações governamentais porque muitas organizações governamentais estão presentes no setor de 'Serviços públicos'.

**Conclusão do Van Dongen**

Esta pesquisa investigou quais e quantas técnicas de segurança de e-mail foram adotadas por organizações na Holanda. Uma lista de organizações holandesas com mais de 10 funcionários (no total 46.650 organizações únicas) foi criada e definimos 19 parâmetros diferentes que foram verificados durante o experimento. Em seguida, usamos a ferramenta 'internet.nl' para verificar se essas técnicas de segurança de e-mail foram adotadas ou não.

Com base nos resultados, descobriu-se que uma organização adotou em média 8,66 de um total de 19 parâmetros. Isso significa que os servidores de e-mail de organizações holandesas adotaram menos de 50% das técnicas de segurança de e-mail definidas pelo governo holandês. Não encontramos uma relação entre o tamanho de uma organização ou a localização geográfica em termos de taxa de adoção. No entanto, encontramos uma relação entre o tipo de setor. O setor de 'Serviços Públicos' tem a pontuação mais alta, com uma pontuação média de 13,18. Assumimos que a pontuação mais alta está relacionada a políticas obrigatórias para organizações governamentais porque muitas organizações governamentais estão presentes no setor de 'Serviços públicos'.

**Resumo do Rafael Santos Reis**

DNSSEC: ASPECTOS GERAIS DE SEGURANÇA, EFICIÊNCIA E ESTATÍSTICAS DE USO NO CONTEXTO BRASILEIRO

Autores: Rafael Santos Reis e Leonardo Santiago Spíndula Thomaz

Orientadora: Professora Dra. Edna Dias Canedo

Co-orientador: Professor Dr. Laerte Peotta

Trabalho de Conclusão de Curso em Engenharia de Redes de Comunicação

Brasília, 23 de Junho de 2015.

Este trabalho estuda o funcionamento dos sistemas DNS e DNSSEC, além de analisar alguns aspectos desses mecanismos, tais como desempenho, eficiência, estatísticas de uso e fraudes, incluindo técnicas de segurança em redes locais. O DNS é um dos principais pilares da Internet. Ataques bem-sucedidos a servidores responsáveis por este serviço podem gerar grandes prejuízos para empresas e até mesmo para usuários finais comuns. O estudo dos mecanismos DNS e DNSSEC é de fundamental importância para garantir as imunidades a esses sistemas e assegurar o bom funcionamento da Internet. Além disso, abordaremos conceitos gerais relacionados a segurança de redes, mencionando o funcionamento dos principais ataques e como evitá-los. Experimentos serão realizados a fim de evidenciar vunerabilidades do DNS que podem ser corrigidas pelo DNSSEC, além de uma metodologia de detecção de malware através do DNS.

**Conclusão do Rafael Santos Reis**

O DNS é um protocolo que tornou mais amigável e gerenciável o acesso aos diversos hosts da Internet, já que é inviável a memorização de IPs. Seu funcionamento tornou-se vital para a grande rede e para todas as redes locais.

Como quase todos os protocolos de rede, o DNS está vulnerável a diversos ataques e incidentes de segurança. Portanto é essencial incrementar segurança neste sistema. Existem muitas medidas que podem ser tomadas para deixar este serviço mais seguro. Habilitar o DNSSEC, além de manter o software de DNS sempre atualizado, é a melhor maneira de prover segurança para a resolução de nomes.

Por todos os benefícios de segurança que o DNSSEC fornece, é altamente indicado o estudo de sua implementação principalmente em um ambiente de alta criticidade, onde a integridade e autenticidades das informações são requisitos importantes.

Por meio da primeira atividade experimental, foi possível notar a efetividade do DNSSEC na proteção das transações de resolução de nomes. Foi exposto também o quão simples é a sua implementação em servidores recursivos, o que pode encorajar mais administradores a aderirem esta extensão segura, já que o sucesso do DNSSEC está diretamente associado à sua disseminação. Neste experimento também foi demonstrado que apesar da segurança contra alguns ataques, o DoS não pode ser evitado com este mecanismo, inclusive o efeito pode ser amplificado, já que o DNSSEC traz consigo uma carga um pouco mais de dados em cada requisição.

No cenário brasileiro em geral, as estatísticas não são muito boas em relação do DNS em geral, não só pelo fato de existir apenas 13,5 % de uso de DNSSEC no recursivos, mas pela quantidade de Servidores abertos para internet sem necessidade e pelos softwares desatualizados que ainda são usados em alguns servidores.

Dado este cenário, pode-se sugerir algumas políticas de segurança a nível nacional para melhorar estes aspectos. A principal delas seria a obrigatoriedade de uso do DNSSEC para um número maior de domínios, assim como já é feito para o domínio de bancos e “.jus”. Como foram detectados servidores de DNS abertos desnecessariamente, seria interessante uma intervenção do governo junto às operadoras para filtrar corretamente a porta 53 na internet, já que hospedar um serviço de DNS é dispensável para a grande maioria dos clientes de internet, que muitas vezes possuem inconscientemente um servidor disponível. 53

A administração do DNSSEC em servidores autoritativos pode trazer alguma complexidade, e isso explica por que é tão pouco utilizado. Já no caso dos servidores recursivos, não há nenhuma dificuldade em sua implementação e manutenção.

Em um trabalho futuro, poderia ser considerado a configuração de um servidor DNS aos modelos de um "honey pot", desta maneira poderia ser alimentada uma base de IPs maliciosos, e poderiam ser estudados novas vulnerabilidades que envolvem o DNS.

**Resumo Liang Zhu**

A estrutura DANE (autenticação baseada em DNS de entidades nomeadas) usa DNSSEC para fornecer uma fonte de confiança e, com a TLSA, pode servir como uma raiz de confiança para certificados TLS. Isso serve para complementar os métodos tradicionais de autenticação de certificado, o que é importante devido aos riscos inerentes à confiança em centenas de organizações - riscos já demonstrados com vários comprometimentos. O protocolo TLSA foi publicado em 2012, e este artigo apresenta o primeiro estudo sistemático de sua implantação. Estudamos o uso de TLSA, desenvolvendo uma ferramenta que analisa ativamente todas as zonas assinadas em .com e .net em busca de registros TLSA. Descobrimos que o uso de TLSA é precoce: em nossa última medição, das zonas com sinal de 485k, encontramos apenas 997 nomes de TLSA. Nós caracterizamos como ele está sendo usado até agora e descobrimos que cerca de 7–13% dos registros TLSA são inválidos. Descobrimos que 33% das respostas TLSA são maiores do que 1.500 bytes e muito provavelmente serão fragmentadas.

**Conclusão Liang Zhu**

Embora estudemos dois dos maiores TLDs (.com e .net), eles são apenas um subconjunto da Internet. Alguns outros TLDs têm tantas ou mais delegações assinadas; no entanto, esses arquivos de zona de ccTLDs geralmente não estão disponíveis. Acreditamos que os dados que estudamos são grandes o suficiente para fornecer uma visão geral da implantação atual do DANE TLSA. Não sabemos de qualquer tendência no subconjunto que medimos.

Nosso conjunto de dados é grande: em 3 de dezembro de 2014, havia 115,2 milhões e 15,1 milhões de zonas ativas em .com e .net, respectivamente [34,36].

Em segundo lugar, investigamos todas as subzonas assinadas por DNSSEC desses dois TLDs, extraindo todos os registros DS nos arquivos de zona. Em 3 de dezembro de 2014, investigamos 405 mil zonas .com assinadas por DNSSEC e 79 mil zonas .com assinadas [35]. Só investigamos zonas assinadas por DNSSEC porque DANE depende de DNSSEC para integridade. Embora um registro TLSA possa ser colocado em zonas não assinadas por DNSSEC, esses registros não são eficazes porque não possuem a verificação de integridade fornecida pelo DNSSEC.

Terceiro, exploramos três principais serviços seguros (HTTPS, SMTP e XMPP) que têm maior probabilidade de usar registros TLSA. Outros serviços que usam TLS são aplicativos VPN e SIP. No entanto, não sabemos de nenhuma implantação usando DANE TLSA para eles.

Este artigo apresenta a primeira medição da implantação do DANE TLSA. Os principais resultados são resumidos a seguir. A autenticação de certificado baseada em CA atual funciona bem na maioria dos casos e as pessoas não sentem a necessidade de usar um protocolo de autenticação completamente novo, embora o DANE forneça vários benefícios, como redução da superfície de ataque e criação de extensões seguras / multifuncionais de correio da Internet (S / MIME ) possível implantação global [25]. Nossa medição mostra que o uso de DANE TLSA é precoce. No entanto, surge a tendência crescente de implantação de DANE TLSA. Nossa validação TLSA mostra que a implantação atual do DANE tem inconsistência de segurança. Entre os registros TLSA encontrados, há consistentemente cerca de 7% - 13% dos registros TLSA incompatíveis com os certificados do servidor ao longo do tempo de nossa observação. Observamos que o uso mais comum (71% -84%) do registro TLSA é: certificado emitido por domínio correspondente a certificados completos com SHA-256. Encontramos 33% das respostas TLSA sofrendo fragmentação de IP, resultando em ataques de fragmentação e latência adicional de processamento de consulta.

Nosso sistema de monitoramento PryDane está continuamente em execução para acompanhar a nova implantação do DANE. Estamos trabalhando no lançamento do código-fonte. (O pseudocódigo é mostrado na Figura 2.) Estamos explorando diferentes serviços que levam a registros TLSA implantados no DNS, além de SMTP e HTTPS. Também estamos estendendo PryDane para capturar outros casos DANE possíveis, como OPENPGPKEY [39], e adicionando validação de certificado IPv6. Nossas medições atuais cobrem .com e .net com acesso direto às zonas; trabalhos futuros podem explorar outras zonas assinadas por DNSSEC ou análise DNS passiva de TLSA.

**Resumo Pawel Szalachowski and Adrian Perrig**

Embora o Sistema de Nomes de Domínio (DNS) tenha sido projetado como um sistema de nomenclatura, seus recursos o tornaram atraente para redefini-lo para a implantação de novos sistemas. Uma classe importante de tais sistemas são os aprimoramentos de segurança e esse trabalho esclarece sua implantação. Mostramos as características dessas soluções e medimos a confiabilidade do DNS nesses aplicativos. Investigamos a compatibilidade dessas soluções com a rede Tor, sinalizamos as mudanças necessárias e relatamos desvantagens surpreendentes na resolução DNS do Tor.

**Conclusão Pawel Szalachowski and Adrian Perrig**

Nosso estudo confirma que os aprimoramentos de segurança baseados no DNS devem respeitar o limite conservador de 512 bytes para respostas, já que a robustez do transporte do DNS pode ser influenciada por muitos fatores incontroláveis. Felizmente, o limite é suficiente para cerca de 95% de todas as respostas recebidas. No entanto, nosso estudo não confirma a crença comum de que TXT RRs estão sendo discriminados.

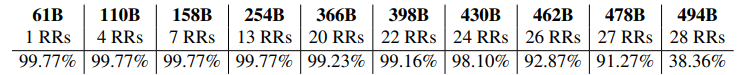


Tabela 4: Fração de resoluções bem-sucedidas (ou seja, único A RR retornado) dependendo do tamanho da resposta (do servidor autorizado).

Nosso trabalho identifica a resolução DNS no Tor como um assunto interessante para trabalhos futuros, pois a achamos surpreendente e inconsistente: os resolvedores não retornam grandes respostas, lidam de maneira ligeiramente diferente com PTR RRs para endereços IPv4 e IPv6, AAAA RRs são oficialmente suportados, mas na prática são resolvidos por apenas 23% de todos os resolvedores. Também observamos que restringir outros RRs (especialmente relacionados a PKI, como TLSA) na verdade diminuirá a segurança dos usuários finais. Portanto, para cumprir a missão do Tor (ou seja, "permitir que as pessoas melhorem sua privacidade e segurança na Internet"), os desenvolvedores devem considerar o suporte a aprimoramentos de segurança baseados em DNS.

**Resumo GEORGIOS KAMBOURAKIS**

Com centenas de bilhões de emails enviados diariamente, a adoção de padrões contemporâneos de segurança de email e melhores práticas pelos respectivos provedores é de extrema importância para todos nós. Deixando de lado as medidas dependentes do usuário, digamos, S / MIME e PGP, este trabalho concentra-se nos atuais padrões de segurança adotados na prática pelos provedores para salvaguardar as comunicações entre seus servidores SMTP. Para isso, desenvolvemos uma ferramenta não intrusiva cunhada MECSA, que está publicamente disponível como um serviço de aplicação web para quem deseja avaliar instantaneamente o status de segurança de seu provedor de e-mail em relação aos canais de comunicação de entrada e saída. Capitalizando os dados coletados pela MECSA ao longo de um período de 15 meses, ou seja, ≈7.650 avaliações, analisando um total de 3.236 provedores de e-mail únicos, detalhamos a taxa de adoção de extensões de segurança de e-mail de última geração, incluindo STARTTLS, SPF, DKIM, DMARC e MTA-STS. Nossos resultados indicam um claro aumento nas conexões criptografadas e no uso de SPF, mas também um retardo considerável na taxa de penetração do restante dos padrões. Esse atraso é ainda mais agravado pela prevalência ainda baixa de DNSSEC, que também é avaliada para o espaço de segurança de e-mail no contexto deste trabalho.

**Conclusão GEORGIOS KAMBOURAKIS**

A adoção de padrões modernos de segurança de e-mail para comunicações MTA a MTA não é obrigatória até agora. Conseqüentemente, um provedor de e-mail pode atingir um grau justo de interoperabilidade com outros provedores sem necessariamente suportar padrões de segurança de última geração e melhores práticas [62]. Para o leitor interessado, uma análise sutil dessa interoperabilidade versus troca de segurança é fornecida em [54]. Pior ainda, essa falta de incentivos claros que estimulam a adoção de fortes medidas de segurança se propaga inevitavelmente ao longo da cadeia de abastecimento. De fato, essa assertiva foi verificada pelos autores em [51]. Do ponto de vista do usuário final, esta situação é duplamente problemática, porque nem eles têm os meios de saber se e até que ponto tais padrões são implementados por seu provedor nos bastidores, nem suas comunicações por e-mail estão adequadamente protegidas em todos os saltos de rede possíveis. Eles até sofrem, digamos, de surtos de e-mails em massa não solicitados devido a essa mesma deficiência.

Este trabalho tem um duplo propósito. Primeiro, desenvolvemos uma plataforma de avaliação de e-mail que vem em dois sabores; O MECSA pode ajudar tanto o usuário comum quanto os administradores de sistemas de e-mail, enquanto o MECSA-ST pode ser de interesse para pesquisadores que trabalham nesta área. O cerne da questão aqui é que, para estimular melhorias, neste caso no status quo de segurança dos provedores de e-mail, deve-se ser capaz de avaliá-lo de forma direta e maciça. Em segundo lugar, capitalizamos os dados abundantes e diversos coletados por nossa plataforma para realizar uma avaliação oportuna em grande escala do estado da situação nesta área, com foco em sete padrões de segurança diferentes. Vis-à-vis o trabalho relacionado, os resultados deste esforço são muito mais completos, uma vez que eles dizem respeito a ambos os fluxos de comunicação e, adicionalmente, consideram os padrões mais novos ou outros aspectos que não foram abordados por trabalhos anteriores nesta área. Os resultados obtidos são bifacetados. Por um lado, eles revelam carências ou soluços significativos na implementação de alguns desses padrões, com DNSSEC e MTA-STS se destacando por diferentes motivos. O DNSSEC afeta diretamente todos os outros padrões, exceto o MTA-STS e, portanto, é um fator-chave para o fornecimento de segurança real no ecossistema de e-mail. Por outro lado, também testemunhamos resultados favoráveis, especialmente para STARTTLS, incluindo o uso de cifras de criptografia fortes.

No momento, estamos trabalhando para fornecer melhorias adicionais à plataforma MECSA, incluindo o suporte para os padrões emergentes SMTP TLS Reporting [63] e RequireTLS [64].

**Resumo Dennis Tatang**

Hoje em dia, o e-mail ainda é o canal de comunicação mais popular da Internet. É baseado no protocolo SMTP (Simple Mail Transfer Protocol), que carece de propriedades básicas de segurança, como confidencialidade e autenticidade, apesar de sua importância cada vez maior. Isso resulta em spam e frequentes ataques de phishing, geralmente com endereços de e-mail de remetentes falsificados para parecerem mais confiáveis, bem como transmissões não criptografadas por padrão. Para resolver esses problemas conhecidos, protocolos adicionais, como STARTTLS, foram desenvolvidos. STARTTLS habilita a criptografia de transporte com Transport Layer Security (TLS) para sessões SMTP entre dois servidores de e-mail. No entanto, um invasor pode tirar vantagem do fato de que a criptografia é oportunista e o comando STARTTLS é enviado de forma simples. Portanto, ele pode ser retirado da comunicação, resultando em uma inevitável transmissão de texto simples da própria mensagem de e-mail. Esse ataque é conhecido como downgrade de TLS. O novo protocolo MTA-STS (Mail Transfer Agent Strict Transport Security) visa prevenir downgrades de TLS para sessões SMTP de entrada. Neste artigo, conduzimos o primeiro estudo de medição longitudinal em larga escala sobre a adoção do MTA-STS. Mostramos que ele é ativado em 0,0124% de 1,76 milhão de domínios escaneados, com um limite inferior de 45,4% para o crescimento da taxa de adoção em cinco meses.

**Conclusão Dennis Tatang**

Neste trabalho, medimos a distribuição de um protocolo de segurança jovem (MTASTS) pela primeira vez. Mostramos que o uso é bastante baixo, ocorrem erros de configuração e discutimos que o MTA-STS provavelmente já está obsoleto devido ao uso comparativamente difundido do DANE. Para trabalhos futuros, a adoção de MTASTS deve ser investigada e comparada com a distribuição de DANE.

**Resumo Ralph Holz**

O e-mail e o bate-papo ainda constituem a maioria das comunicações eletrônicas na Internet. A padronização e aceitação de protocolos como SMTP, IMAP, POP3, XMPP e IRC permitiu implantar servidores para e-mail e chat de forma descentralizada e interoperável. Esses protocolos podem ser protegidos fornecendo criptografia com TLS - diretamente ou por meio da extensão STARTTLS. PKIs X.509 e métodos ad hoc podem ser aproveitados para autenticar pares de comunicação. No entanto, a configuração segura não é direta e muitas combinações de mecanismos de criptografia e autenticação levam a implantações inseguras e, potencialmente, ao comprometimento dos dados em trânsito. Neste artigo, apresentamos o maior estudo até o momento que investiga a segurança de nossas infraestruturas de e-mail e chat. Usamos varreduras ativas em toda a Internet para determinar a quantidade de implantações de serviço seguras e empregamos monitoramento passivo para investigar em que grau os agentes de usuário realmente escolhem mecanismos seguros para sua comunicação. Abordamos as interações cliente-servidor e também o encaminhamento servidor-a-servidor. Além dos mecanismos de autenticação e criptografia que os protocolos investigados oferecem na camada de transporte, também investigamos os métodos de autenticação de cliente em uso na camada de aplicação. Nossas descobertas lançam luz sobre uma área ainda não explorada da Internet. Nossos resultados, em poucas palavras, são uma mistura de descobertas positivas e negativas. Embora os grandes provedores ofereçam boa segurança para seus usuários, a maior parte de nossa comunicação é mal protegida em trânsito, com pontos fracos na configuração criptográfica e especialmente na escolha dos mecanismos de autenticação. Apresentamos uma lista de mudanças acionáveis para melhorar a situação.

**Conclusão Ralph Holz**

Este documento apresentou o maior estudo sobre a segurança da infraestrutura padrão de mensagens da Internet até o momento. Com base em varreduras ativas de servidores e monitoramento passivo de conexões de clientes, coletamos os parâmetros usados para estabelecer sessões SSL / TLS, os detalhes de certificados X.509 oferecidos por servidores e os métodos de autenticação de camada de aplicativo oferecidos e usados por, clientes. Em toda a Internet, encontramos um número preocupantemente alto de servidores mal protegidos. Isso ocorreu devido a parâmetros criptográficos e escolhas de cifras ou devido a material criptográfico inválido ou duplicado. Muitos servidores também oferecem métodos de autenticação de camada de aplicativo fracos. O lado bom é que há implantações significativamente melhores nos serviços mais populares e a maioria dos clientes observados se conectam usando parâmetros razoavelmente seguros quando solicitam a criptografia. No entanto, muitas das conexões que observamos ainda foram realizadas sem proteção. Além disso, descobrimos que muitas configurações de cliente para servidor, especialmente para SMTP, não usavam credenciais válidas. Isso significa que o e-mail em trânsito pode muitas vezes ser entregue por meio de saltos não criptografados e não autenticados. Fornecemos uma lista de recomendações que são acionáveis e podem ajudar a melhorar significativamente a situação.