Plano de Trabalho de Conclusão de Curso
Análise do Ecossistema DANE para E-mail na Internet Brasileira

UDESC - Centro de Ciências Tecnológicas
Departamento de Ciência da Computação
Bacharelado em Ciência da Computação - Integral
Turma 2021/1 - Joinville – Santa Catarina

Matheus Rambo da Roza – matheusrambo97@gmail.com
Orientador: Rafael Rodrigues Obelheiro – rafael.obelheiro@udesc.br

Resumo - O SMTP (Simple Mail Transfer Protocol), o protocolo usado para transporte de correio eletrônico na Internet, não usa criptografia nativa, e por isso não garante confidencialidade, integridade ou autenticação do tráfego. Mecanismos para garantir a segurança do SMTP foram propostos, sendo um dos principais o STARTTLS, que permite o uso de canais criptografados TLS (Transport Layer Security) em transações SMTP. O STARTTLS exige que clientes e servidores SMTP tenham certificados digitais, usualmente emitidos por autoridades certificadoras (ACs). O DANE (DNS-based Authentication of Named Entities) é um padrão da Internet que permite que certificados TLS sejam autenticados usando registros TLSA publicados no DNS pelos donos desses certificados, dispensando a necessidade de autoridades certificadoras. O principal caso de uso do DANE atualmente está na validação dos certificados TLS usados para proteção do tráfego SMTP. Este trabalho propõe realizar um estudo de medições sobre o uso de DANE para proteção do serviço de e-mail na Internet brasileira, identificando a adoção do DANE em domínios brasileiros e analisando se o padrão está sendo usado corretamente. Para isso, pretende-se replicar a metodologia proposta por um trabalho anterior, que realizou um estudo análogo com os domínios genéricos `.com`, `.net` e `.org`, e com os domínios nacionais `.nl` e `.se`.

Palavras-chave: *Protocolos de segurança, DANE, Transport Layer Security, Autoridade de certificação, SMTP.*

1. Introdução e Justificativa

O correio eletrônico, um dos serviços mais populares da Internet, tradicionalmente não oferece garantias de segurança. O transporte de e-mail é realizado pelo protocolo SMTP (Simple Mail Transfer Protocol) (KLENSIN, 2008), que não possui mecanismos criptográficos nativos. O STARTTLS (HOFFMAN, 2002) (DUKHOVNI, 2014) é uma extensão para o SMTP que permite que servidores estabeleçam uma sessão TLS (Transport Layer Security) (RESCORLA, 2018) para garantir confidencialidade, integridade e autenticação do tráfego SMTP. O STARTTLS oferece um mecanismo criptográfico dito oportunista (DUKHOVNI, 2014): no início de uma sessão SMTP não criptografada, os servidores podem negociar o estabelecimento da sessão TLS, desde que ambos suportem essa opção. Existem dois problemas principais associados ao STARTTLS (BAATEN, 2019):

1. Ataque de *downgrade*: como os pares trocam informações dentro de uma sessão SMTP desprotegida para saber se podem ou não iniciar uma sessão TLS, um atacante capaz de realizar um ataque de homem no meio (*man-in-the-middle*, MITM) pode simplesmente eliminar as mensagens que sinalizam o suporte a STARTTLS para forçar o uso de SMTP sem criptografia, sem que seja possível detectar essa supressão.

2. Redirecionamento de tráfego: como normalmente a autenticidade dos certificados TLS dos servidores de e-mail não é validada, um atacante capaz de realizar um MITM pode fornecer um certificado forjado e com isso interpor-se entre os servidores, violando as propriedades de segurança do TLS.

Uma solução para esses problemas é a adoção do padrão DANE para SMTP (DUKHOVNI e HARDAKER, 2015), que usa registros TLSA no DNS (HOFFMAN E SCHLYTER, 2012) para sinalizar de forma segura que um servidor de e-mail suporta STARTTLS e para publicar informações que permitem que servidores SMTP validem os certificados TLS recebidos durante o estabelecimento de uma sessão TLS. Com isso, as ameaças mencionadas acima são mitigadas.

O DANE (DNS-based Authentication of Named Entities) (HOFFMAN E SCHLYTER, 2012) (DUKHOVNI e HARDAKER, 2015), permite que o responsável por um domínio DNS publique um registro TLSA com informações sobre o certificado TLS usado por um dado servidor, como um servidor HTTPS ou SMTP+STARTTLS. A integridade e a autenticidade do registro TLSA são garantidas pelas extensões de segurança do DNS (DNSSEC) (ARENDS et al., 2005). Os certificados publicados via DANE são emitidos pelo próprio servidor TLS, sem depender de uma autoridade certificadora (AC); isso mitiga uma ameaça clássica da infraestrutura de chaves públicas (PKI) do TLS, que é a possibilidade de que uma AC emita certificados válidos para qualquer nome (CLARK e OORSCHOT, 2013). Assim, para validar um certificado TLS apresentado por um servidor, um cliente pode (1) obter o registro TLSA do servidor, (2) validar esse registro usando as assinaturas do DNSSEC, e (3) verificar se o certificado é consistente com o registro TLSA.

O DANE só pode funcionar corretamente quando todos os principais cumprem suas responsabilidades, são eles: servidores TLS apresentando certificados, servidores DNS que publicam registros TLSA, clientes DNS validando respostas DNS usando DNSSEC e clientes TLS verificando certificados usando registros TLSA. Infelizmente, a complexidade do DANE leva a muitas oportunidades de erros de configuração. Por exemplo, no lado do servidor, podem conter erros DNSSEC nos registros TLSA, como assinaturas expiradas ou os certificados serem inconsistentes com os registros TLSA publicados. Já no lado do cliente, os resolvedores de DNS podem não validar os registros TLSA adequadamente ou aplicativos TLS com erros, de modo que não se preocupam em verificar a validade dos certificados (LEE, 2020).

Para entender o estado atual do ecossistema DANE para e-mail na Internet, Lee (2020) realizou um estudo de medições envolvendo os domínios de segundo nível sob os domínios genéricos `.com`, `.net` e `.org`, e sob os domínios nacionais `.nl` e `.se` (respectivamente Holanda e Suécia). Ao longo de 24 meses, foram coletados dados sobre registros MX (que indicam servidores de e-mail) e TLSA publicados nesses domínios, e também os certificados TLS apresentados pelos servidores SMTP encontrados. O estudo descobriu que 35% dos registros TLSA não podiam ser validados por conta de registros DNSSEC ausentes ou incorretos, e que 3.7% dos certificados eram

inconsistentes com os registros TLSA correspondentes. O estudo também analisou aspectos do SMTP+DANE do ponto de vista do cliente, constatando que, apesar dos padrões serem suportados por software DNS e SMTP de código aberto, eles ainda são pouco adotados por provedores populares de e-mail. As ferramentas e conjunto de dados usados no estudo de (LEE, 2020) estão todas disponíveis através do link `https://dane-study.github.io/`.

Não existem atualmente dados disponíveis sobre a adoção de DANE para e-mail na Internet brasileira. O domínio `.br` não aparece nas estatísticas sobre SMTP+DANE (KNUBBEN, 2021). Este trabalho de conclusão de curso visa a preencher esta lacuna, replicando o estudo de (LEE, 2020) para o domínio `.br`. O objetivo primário é entender a adoção do DANE para proteção de e-mail na Internet. Um objetivo secundário é testar a reprodutibilidade dos artefatos disponibilizados por (LEE, 2020). A reprodutibilidade tem sido um aspecto destacado e valorizado para promover pesquisa científica de qualidade (VITEK e KALIBERA, 2011) (PENG, 2011).

2. Objetivos

Objetivo Geral

Este trabalho tem como objetivo realizar um estudo de medições sobre o ecossistema do DANE para e-mail na Internet brasileira.

Objetivos Específicos

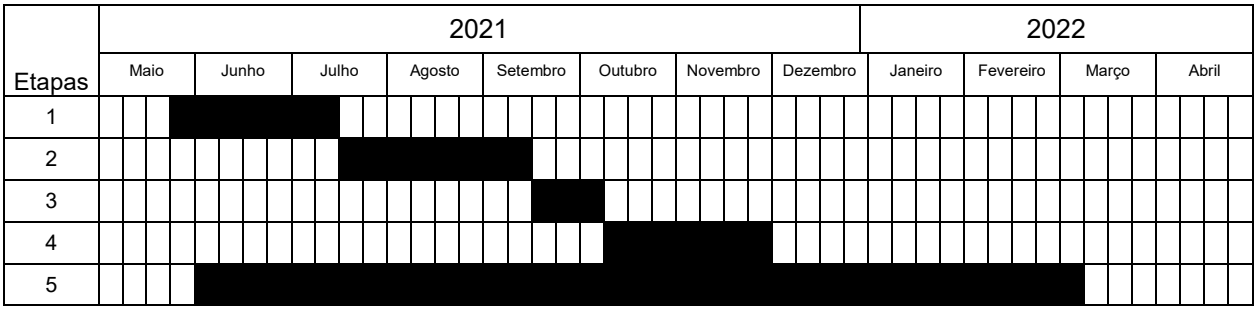
- Realizar uma revisão bibliográfica abrangendo DNS, DANE, e-mail e trabalhos relacionados;
- Replicar a infraestrutura de medições disponibilizada por [Lee 2020] em um ambiente local;
- Coletar dados sobre o uso do DANE na Internet brasileira;
- Analisar os dados coletados.

3. Metodologia

Visando a realização dos objetivos propostos na Seção 2, as atividades foram divididas da seguinte forma:

1. Revisão Bibliográfica;
2. Replicar a infraestrutura de medições em ambiente local;
3. Coletar os dados;
4. Análise dos dados;
5. Escrita da monografia.

4. Cronograma Proposto



5. Linha e Grupo de pesquisa

Este trabalho de conclusão de curso se enquadra no Grupo de Redes e Aplicações Distribuídas (GRADIS), na linha de pesquisa de Segurança Computacional.

6. Forma de Acompanhamento/Orientação

O acompanhamento e orientação das atividades será dado através de encontros semanais e caso necessário, através de encontros não previamente agendados.

7. Referências Bibliográficas

Baaten, Dennis. Better mail security with DANE for SMTP. Apnic, 2019. Disponível em: https://blog.apnic.net/2019/11/20/better-mail-security-with-dane-for-smtp/ . Acesso em: 31 maio 2021.

Clark, Jeremy; Oorschot, Paul C. van. SoK: SSL and HTTPS: Revisiting past challenges and evaluating certificate trust model enhancements. IEEE Symposium on Security and Privacy. 2013. Disponível em: http://www.css.csail.mit.edu/6.858/2020/readings/sok-ssl-https.pdf. Acesso em: 20 maio 2021.

Dukhovni, V. (2014). Opportunistic Security: Some Protection Most of the Time. RFC 7435. https://datatracker.ietf.org/doc/html/rfc7435.

Dukhovni, V., and Hardaker W. (2015). SMTP Security via Opportunistic DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS). RFC 7672. https://datatracker.ietf.org/doc/html/rfc7672.

Dukhovni, V., and Hardaker W. (2015). The DNS-Based Authentication of Named Entities (DANE) Protocol: Updates and Operational Guidance. RFC 7671. https://datatracker.ietf.org/doc/html/rfc7671.

Hoffman, P., and Schlyter, J. (2012). The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA. RFC 6698. https://datatracker.ietf.org/doc/html/rfc6698.

Hoffman, P. (2002). SMTP Service Extension for Secure SMTP over Transport Layer Security. RFC 3207. https://datatracker.ietf.org/doc/html/rfc3207.

H. Lee, A. Girish, R. van Rijswijk-Deij, T. Kwon and T. Chung. A Longitudinal and Comprehensive Study of the DANE Ecosystem in Email. Usenix Security'20, 2020. Disponível em: https://taejoong.github.io/pubs/publications/lee-2020-dane.pdf.

Klensin, J. (2008). Simple Mail Transfer Protocol. RFC 5321. https://datatracker.ietf.org/doc/html/rfc5321.

Knubben , Bart. Overwiew of outbound DANE for SMTP support. 26 maio 2021. Disponível em: https://github.com/baknu/DANE-for-SMTP/wiki/4.-Adoption-statistics. Acesso em: 31 maio 2021.

Peng, Roger. Reproducible Research in Computacional Science. American Association for the Advancement of Science. 2011. Disponível em: https://science.sciencemag.org/content/334/6060/1226/tab-pdf. Acesso em: 25 maio 2021.

Arends, R., Austein, R., Larson, M., Massey, D. and Rose, S. DNS Security Introduction and Requirements. RFC 4033, IETF, 2005. http://www.ietf.org/rfc/rfc4033.txt.

Arends, R., Austein, R., Larson, M., Massey, D. and Rose, S. Resource Records for the DNS Security Extensions. RFC 4034, IETF, 2005. http://www.ietf.org/rfc/rfc4034.txt.

Arends, R., Austein, R., Larson, M., Massey, D. and Rose, S. Protocol Modifications for the DNS Security Extensions. RFC 4035, IETF, 2005. http://www.ietf.org/rfc/rfc4035.txt.

Rescorla, E. (2018). The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446. https://datatracker.ietf.org/doc/html/rfc8446.

Vitek, Jan; Kalibera, Tomas. Repeatability, Reproducibility and Rigor in Systems Research. Institute of Electrical and Eletronics Engineers. 2011. Disponível em: https://ieeexplore.ieee.org/abstract/document/6064509. Acesso em: 25 maio 2021.

_____	_____
Rafael Rodrigues Obelheiro	***Matheus Rambo da Roza***