Plano de Trabalho de Conclusão de Curso
Reprodutibilidade de Estudo Sobre o Protocolo DANE em E-mail no Cenário Brasileiro

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 uso da internet vem a cada dia aumentando, em 2009 apenas 40% da população brasileira a usava, hoje temos mais de 70% dos brasileiros conectados. Com todo esse crescimento no mundo da tecnologia e da internet, vem a preocupação da segurança dos dados de cada um, por isso é que temos os protocolos de segurança. O protocolo que iremos estudar mais a fundo é o DANE (DNS-based Authentication of Named Entities) que é utilizado no TLS (Transport Layer Security - Segurança da Camada de Transporte), o DANE está proposto na RFC 6698 como uma maneira de autenticar entidades de clientes e servidor TLS sem a necessidade de ter uma autoridade de certificação (CA). Desta forma, este trabalho pretende reproduzir o experimento de (Lee, 2020), que realiza um estudo aprofundado sobre o DANE em e-mail, porém em um cenário brasileiro.

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

1. Introdução e Justificativa

O que todos querem ao navegar na internet, realizar uma compra online ou enviar um e-mail é que seus dados estejam sendo enviados de maneira segura, sem nenhuma

fraude ou possível ataque de hackers. Para garantir isso, segundo Lee (2020) é que temos o Transport Layer Security (TLS), responsável por proteger o tráfego da internet em uma variedade de protocolos, como o DNS e HTTP. Simultaneamente com uma infraestrutura de chave pública (PKI), o TLS depende de certificados para vincular entidades às chaves públicas, os quais são emitidos por uma autoridade de certificação (CA). Porém esse modelo de PKI é vulnerável, de maneira que qualquer CA pode emitir certificados para qualquer nome de domínio. Olhando para o passado e conferindo notícias [6, 7] observamos que as CAs emitiram certificados de forma indevida. Com isso, muitos protocolos foram criados afim de resolver essa fraude, porém nenhum deles resolvia o problema de que o processo de validação de um certificado é dependente de uma CA.

Conforme Hoffman (2012), este problema surge porque uma CA comprometida pode emitir certificado de substituição que contém uma chave falsa. Experiências recentes com compromissos de CAs ou seus parceiros de confiança levaram a problemas de segurança muito sérios como os governos de vários países tentando grampear e/ ou subverter os principais sites protegidos por TLS em que milhões de usuários confiam.

Para resolver esta questão, o protocolo de Autenticação de Entidade Nomeadas (DANE) com base em DNS foi proposto para oferecer suporte a TLS sem depender de terceiros confiáveis, como CAs. A princípio, um proprietário de certo nome de domínio que executa um servidor TLS, como HTTPS, ou e-mail seguro via SMTP + STARTTLS, pode publicar suas informações de certificado como um registro DNS chamado de registro TLSA, que pode ser usado por clientes TLS para verificar a autenticidade do certificado de uma forma não PKI. Além disso, a integridade e autenticidade dos registros TLSA são garantidas pelas DNS Security Extensions (DNSSEC) [3, 4, 5].

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 má gestão. 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 não se preocupam em verificar a validade dos certificados (Lee, 2020).

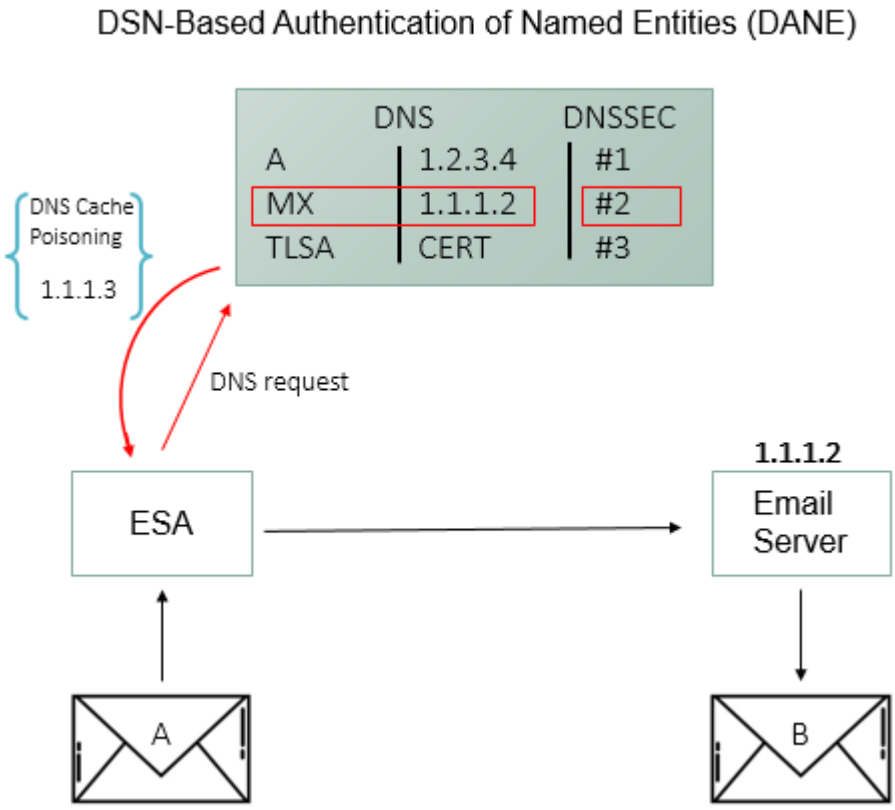

Figura 1: Demonstra um ataque de DNS Cache Poisoning (Envenenamento de Cache DNS). **Fonte:** Autor.

Em resumo, podemos observar na figura 1 como o DANE resolve um ataque de DNS Cache Poisoning e na figura 2 um ataque de Man-In-The-Middle (MITM). Na figura 1 observamos um cliente ‘A’ que irá enviar um e-mail para o cliente ‘B’, o primeiro passo, é nosso e-mail chegar ao EMS (Email Security Appliance – Ferramenta de segurança de e-mail) que precisa saber onde o domínio está localizado através de endereço IP, o segundo passo é fazer uma requisição DNS que responde com o MX (Mail Exchanger). Sem o uso do DANE, o ESA não tem como garantir se esse endereço IP é autêntico, é nesse momento em que ocorre um ataque de envenenamento de cache DNS por um hacker, que irá devolver um endereço IP não autêntico, como no exemplo 1.1.1.3, dessa forma fazendo com que o hacker tenha acesso a todos e-mails. Com o uso do DANE no

nosso ESA, podemos então utilizar a extensão DNSSEC, que adiciona uma nova coluna no DNS records, que nos dá a garantia de que o endereço IP, no caso da figura 1 o IP 1.1.1.2, é o endereço de domínio correto a qual o usuário ‘A’ deseja enviar a mensagem.

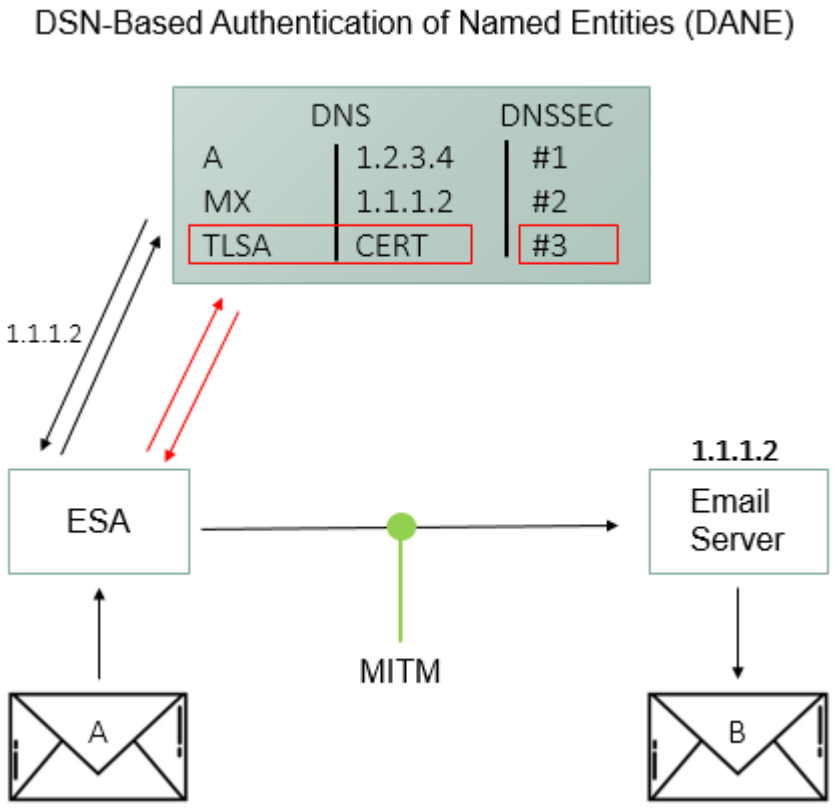

Figura 2: Demonstra um ataque de MITM. **Fonte:** Autor.

Na figura 2, os primeiros passos são semelhantes os que ocorreram na figura 1, ou seja, temos o endereço IP correto para a comunicação com o Servidor de E-mail. Em um ataque MITM, o hacker intercepta o tráfego e tenta remover a criptografia enviando ao ESA uma mensagem dizendo de que não suporta a criptografia e deve ser enviado um texto simples, então o ESA envia um texto simples e o hacker poderá ter acesso aos e-mails. Com o DANE, será checado para esse mesmo domínio, se ele possui um TLSA record e qual é o certificado de publicação, que é garantido pelo DNSSEC se é autêntico ou não. Se o TLSA record existir para esse domínio, temos a garantia de que o servidor de e-mail suporta TLS, ou seja, podemos ter um tráfego criptografado, então caso o mesmo não ocorra, temos a garantia de que temos um MITM, assim podemos abortar a transmissão.

De modo geral, antes do estudo abrangente feito por Lee (2020) não se tinha muito conhecimento sobre o ecossistema DANE para Serviços de E-mail, embora já tivesse um estudo sobre o DANE [6], mas nada relacionado a DANE PKI em SMTP.

O intuito desse estudo é replicar o lado do servidor (Lee, 2020), porém trazendo para os domínios brasileiros, que iremos, a princípio, utilizar alguma lista divulgada na internet. Conforme o andamento do experimento e a coleta de alguns dados concretos, apresentaremos os mesmos ao “Registro.br” para solicitar que eles concedam uma base de dados maior para resultados melhores.

2. Objetivos

Objetivo Geral

Este trabalho tem como objetivo reproduzir um estudo sobre DANE feito por Lee (2020), porém em âmbito brasileiro.

Objetivos Específicos

- Realizar um estudo aprofundado sobre DANE em SMTP, para ter um maior entendimento sobre o funcionamento desses protocolos.
- Formar um banco de dados com uma lista de domínios.
- Adaptar as ferramentas usadas por Lee (2020).
- Realizar experimentos.
- Analisar os dados coletados nos experimentos.

3. Metodologia

4. Cronograma Proposto

5. Linha e Grupo de pesquisa

6. Forma de Acompanhamento/Orientação

7. Referências Bibliográficas

[1] H. Lee, A. Girish, R. van Rijswijk-Deij, T. Kwon and T. Chung. A Longitudinal and Comprehensive Study of the DANE Ecosystem in Email, 2020. https://taejoong.github.io/pubs/publications/lee-2020-dane.pdf

[2] P. Hoffman and J. Schlyter. The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA. RFC 6698, IETF, 2012.

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

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

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

[6] Mozilla piles on China's SSL cert overlord: We don't trust you either. http://bit.ly/1GBPwfG.

[7] Trustwave to escape 'death penalty' for SSL skeleton key. 2012. http://bit.ly/1RbPlNe.

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