SLIDE 1

Apresentação

SLIDE 2

Estrutura da apresentação

SLIDE 3

SLIDE 4

**STARTTLS:** É uma extensão de segurança para SMTP, que adiciona autenticação e confidencialidade na comunicação entre agentes SMTP. Só utilizando o SMTP para envio de email, não possuímos segurança nenhuma. Com STARTTLS um cliente pode estabelecer um canal seguro TLS em uma transação SMTP

**TLS:** O TLS é o protocolo de Segurança da camada de Transporte que nos garante confidencialidade e integridade para as aplicações que usam TCP como HTTP e SMTP

NO EXEMPLO:  
Após o handshake, o servidor identifica com 220 que o cliente pode prosseguir e então o cliente envia o comando EHLO para informar que gostaria de utilizar SMTP.

Então o servidor anuncia com 250 STARTTLS que oferece suporte a STRATTLS.  
O cliente utiliza o comando STARTTLS indicando que gostaria de utilizar o canal seguro e então a negociação TLS é feita.

SLIDE 5

Se utilizarmos somente o STARTTLS, podemos ter dois problemas.  
  
**Vulnerabilidade a um ataque de Downgrade:** Onde um atacante que manipula o tráfego entre o cliente e o servidor, exclui a mensagem que sinaliza o suporte a STARTTLS, forçando o uso de SMTP sem criptografia.

**Validação do certificado TLS:** Ou também conhecido como o **problema de infraestrutura da Chave Pública**. Onde temos Diversas Autoridades Certificadoras que emitem certificados utilizando uma Chave Pública (PKI).

E SE, uma dessas CAs for enganada a assinar um certificado inválido. E SE, uma dessas CAs for **comprometida**, ou seja, se uma dessas CAs tiverem sua chave privada comprometida.

SLIDE 6

A solução para esses problemas é o uso do DANE (DNS-Based Authentication of Named Entities)

É um protocolo de segurança da Internet que permite que os certificados sejam vinculados a nomes de domínio.

Utiliza o DNSSEC para autenticar os registros DNS, como por exemplo o registro TLSA que é um novo registro adicionado pelo DANE, que permite associar um certificado ou uma chave pública a um servidor.

**DNSSEC:** DNSSEC é uma extensão que adiciona propriedades de autenticação e integridade ao DNS.

SLIDE 7

E a grande vantagem de utilizar o DANE é que Ele oferece suporte TLS sem depender de um AC

Isso também é muito bom pois uma AC pode ser comprometida assim gerando outro problema além do STRIPTLS.

Depender de uma AC é um problema pois uma AC pode ser **comprometida**, ou seja, se uma dessas CAs tiverem sua chave privada comprometida.

SLIDE 8

Agora vou mostrar pra vocês uma visão geral de como funciona o DANE junto com DNSSEC e STARTTLS.

1º nosso agente de transporte de email (MTA) busca os registros MX (Servidor de e-mails) para o domínio example.org e também o RRSIG que é onde contém a assinatura digital de um RRset assinado com a chave privada

SLIDE 9

Após isso, o MTA busca então os registros TLSA, a presença do TLSA sinaliza que o MX suporta TLS e caso não possua o registro TLSA, o cliente deve encerrar a conexão.

Em ambos os passos o DNSSEC garante a integridade e autenticidade dos registros DNS recebidos

SLIDE 10 e 11

Nesse passo o comando STARTTLS é utilizado pelo cliente e então o servidor envia o certificado.

SLIDE 12

Agora o certificado que foi recebido é confrontado com os registros TLSA para verificar se pode ser validado ou não.

De maneira mais específica, no registro TLSA, possui um campo “**Dados de associação do certificado**”, que especifica o valor de um certificado ou chave pública.

SLIDE 13

Se tudo estiver correto então, o cliente finaliza o HANDSHAKE TLS com o servidor e o canal TLS é usado para enviar uma ou mais mensagens.

SLIDE 14

Esse é o ecossistema DANE, temos o lado CLIENTE e o lado SERVIDOR.

Para que o ecossistema DANE funcione corretamente, ambas as partes devem funcionar.

SLIDE 15

O objetivo primário....

Como um segundo objetivo também iremos testar a reprodutibilidade do estudo científico feito por LEE (2020). (.com, .net, .org, .nl e .se)

SLIDE 16

Agora irei falar sobre a proposta desse trabalho.

Ela é dividida em 2 etapas: A coleta dos dados e a análise dos mesmos.

Nessa imagem podemos observar essas etapas.

**COLETA DE DADOS**

No passo 1: o coletor DNS (que será desenvolvido) buscando os registros MX para todos os domínios que estão na lista.

No passo 2: o coletor DNS busca então os registros TLSA. Para a garantia de suporte a TLS.

No passo 4: é produzida uma lista dos MXs com registros TLSA correspondentes.

No passo 5: O coletor SMTP através do STARTTLS faz a conexão com os servidores SMTP que devolvem os certificados que serão verificados com os registros TLSA para serem validados.

**ANÁLISE DOS DADOS**

No passo 3: os dados coletados sobre os MXs e os TLSA serão analisados, assim vamos poder verificar quantos MX possuem TLSA e quantos não possuem.

Após a coleta dos dados no passo (6), será possível verificar quais MXs possuem STARTTLS e os que não possuem.

Após a verificação de consistência dos certificados com os TLSAs, obtemos a última coleta de dados no passo (8), esses dados irão nos mostrar quantos domínios estabeleceram um canal TLS com o servidor, tal canal que é utilizado para o envio de mensagens de maneira segura e criptografada.

SLIDE 17

para que a combinação STARTTLS+DANE garanta as propriedades de segurança desejadas, diversos elementos precisam ser configurados corretamente e de forma harmônica, mas que problemas de configuração são comuns na prática

Como não existe nenhum dado sobre o uso do DANE para email na internet brasileira, esse trabalho irá preencher essa lacuna para os domínios .br

SLIDE 18

Cronograma

SLIDE 19

Como etapas futuras então será necessário desenvolver o Crawler/Coletor DNS como comentado la no slide de proposta. Vale ressaltar que estamos vendo a possibilidade de utilizar um crawler DNS que já foi desenvolvido e é disponibilizado pelo projeto ADAM que é vinculado ao NIC.CZ