Bezpečné doručování pošty

Ondřej Caletka

cesnet

14. května 2019

Stručně o elektronické poště

cesnet

Stručně o elektronické poště

- koncepčně vychází z klasické pošty
- jednoduché textové zprávy podle RFC 822/2822/5322
- hlavička jako soubor polí `Klíč: Hodnota`
- tělo zprávy za prázdným řádkem
- omezení na 7bit znaky, 78 na řádek (max. 998)
- rozšíření MIME pro vícedílné zprávy

Povinné hlavičky

```
From: Date: Message-ID:
```

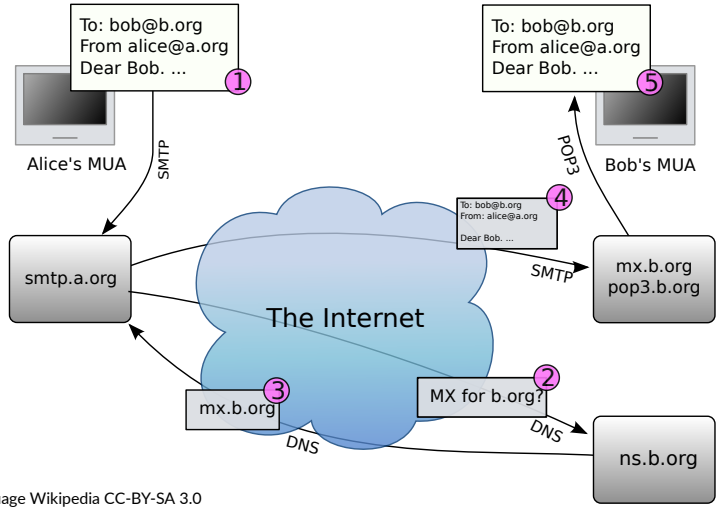
cesnet

Přenos pošty pomocí SMTP

- metoda *ulož a přepošli*
- jednoduchý textový protokol podle RFC 821/2821/5321
- vytváří obálku pro zprávy s novou dvojicí adres *odkud* - *kam*
  - obálková adresa *odkud* slouží k hlášení problémů (nebo i úspěchu) s doručováním
  - obálková adresa *kam* určuje, komu bude zpráva doručena
- předávání zpráv je zaznamenáváno na začátek hlavičky zprávy

cesnet

Princip SMTP



Yzmo at the English language Wikipedia CC-BY-SA 3.0

cesnet

```
220 SMTP server ready
EHLO local.machine.example
250 server.example.net
MAIL FROM:<jdoe@machine.example>
250 2.1.0 Ok
RCPT TO:<mary@example.net>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
From: John Doe <jdoe@machine.example>
To: Mary Smith <mary@example.net>
Subject: Saying Hello
Date: Fri, 21 Nov 1997 09:55:06 -0600
Message-ID: <1234@local.machine.example>

This is a message just to say hello.
.
250 2.0.0 Ok: queued as C5D1822AF6
QUIT
221 2.0.0 Bye
```

cesnet

Autentizační mechanizmy

cesnet

Autentizační mechanizmy

SPF	Autentizace hlavičkové adresy `From:`
DKIM	Elektronické podepisování na straně serveru
DMARC	Pravidla zahození zpráv se zfalšovaným odesílatelem
ARC	Elektronické podepisování hlaviček `Received:`

cesnet

Problém SPF s přeposíláním pošty

Problematické chování

- $\mathbb{A}$ publikuje SPF ve stylu `ip4:… -all`
- $\mathbb{B}$ umožňuje přeposílání došlé pošty
- $\mathbb{C}$ validuje SPF a při *fail* zprávy odmítá

$\mathbb{A}$ posílá poštu do $\mathbb{B}$, ta je následně přeposlána do $\mathbb{C}$
$\mathbb{C}$ vidí poštu od $\mathbb{A}$ doručenou z IP adresy serveru $\mathbb{B}$

Možná řešení

- $\mathbb{A}$ použije *softfail*
- $\mathbb{B}$ přepíše zpáteční adresu
- $\mathbb{C}$ vyhodnotí *fail* stejně jako *softfail*

Sender Rewriting Scheme

- standard přepisování obálkových adres při přeposílání
- přeposílání funguje pouze omezenou dobu
- nelze předem spočítat přepis na libovolnou adresu
  - použitím databáze
  - použitím hashovací funkce

Příklady přepsaných adres

```
SRS0=KKKKKKKK@B.org
SRS0=HHH=TT=A.org=user@B.org
SRS1=KKK=B.org==HHH=TT=A.org=user@B2.org
```

cesnet

Problém DMARC s e-mailovými konferencemi

- stačí aby vyhověl SPF **nebo** DKIM
- přeposílání zpráv zachovává DKIM
- konference ničí DKIM a činí SPF nepoužitelným
  - sice je validní, ale bez vztahu k doméně odesílatele
- konference tedy musí měnit adresu `From:`
  - přinejmenším pro respondenty s DMARC politikou
  - původní adresu přispěvatele je možné přesunout do `Reply-To:`
  - případně je možné zprávy obalit jako MIME Digest o jedné zprávě – problematická podpora MUA

cesnet

Šifrování transportu zpráv

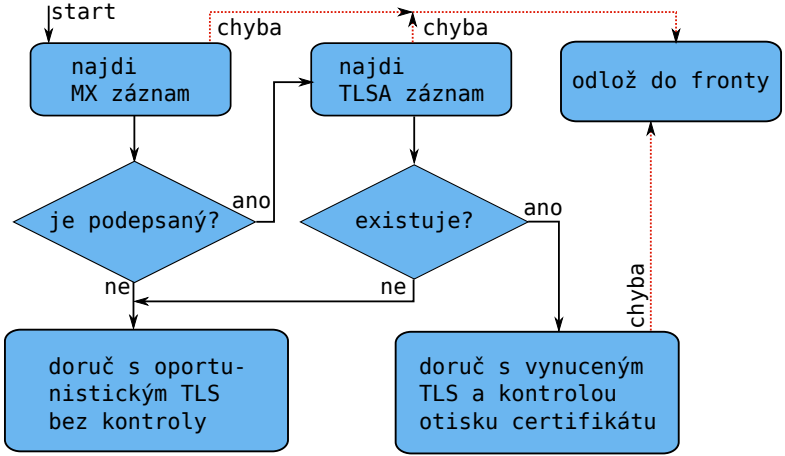
cesnet

Šifrování transportu zpráv

- výchozí nastavení je často SMTP bez TLS
- self-signed certifikát *je dostačující*
- zabezpečené předávání lze vynutit publikací TLSA záznamu s otiskem veřejného klíče v DNS
- validaci DANE při odesílání podporují Postfix a Exim
- je třeba bezpečné spojení s validujícím resolverem

cesnet

Chování validujícího klienta



cesnet

Testujeme nástrojem `posttls-finger`

Bez TLSA záznamu – Untrusted

```
$ /usr/sbin/posttls-finger -c seznam.cz
posttls-finger: mx1.seznam.cz:25: Matched subjectAltName: mx1.seznam.cz
posttls-finger: certificate verification failed for mx1.seznam.cz:25:
                untrusted issuer /C=US/O=thawte, Inc./OU=Certification
                Services Division/OU=(c) 2006 thawte, Inc. - For
                authorized use only/CN=thawte Primary Root CA
posttls-finger: Untrusted TLS connection established to mx1.seznam.cz:25:
                TLSv1.2 with cipher AES128-SHA (128/128 bits)
^^I^^I
```

S TLSA záznamem – Verified

```
$ /usr/sbin/posttls-finger -c cesnet.cz
posttls-finger: using DANE RR: _25._tcp.… IN TLSA 2 0 1 5C:42:8B:01:3B:2E:3F:0D:30…
posttls-finger: postino.cesnet.cz:25: depth=1 matched trust anchor certificate
                sha256 digest 5C:42:8B:01:3B:2E:3F:0D:30…
posttls-finger: Verified TLS connection established to postino.cesnet.cz:25:
                TLSv1 with cipher DHE-RSA-AES256-SHA (256/256 bits)
^^I^^I
```

cesnet

Co děláme na CESNETu

cesnet

Co děláme na CESNETu

- SPF nepublikujeme, částečně validujeme
- DKIM používáme
- DMARC nepublikujeme, nevalidujeme
- používáme certifikáty od TCS na poštovních serverech
- publikujeme TLSA záznamy
- validujeme TLSA při odesílání pošty

cesnet

Jak odesílat poštu

- přímo z příslušného serveru
- validní hostname, reverzní záznam
- odesílat z funkční adresy
- volitelně DKIM podpis
- přeposílání přes *smart relay není nezbytné*

cesnet

Děkuji za pozornost

Ondřej Caletka
Ondrej.Caletka@cesnet.cz
https://**Ondřej.Caletka.cz**

Prezentace je již nyní k dispozici ke stažení.