

Bezpečnější pošta *aneb DANE for SMTP*

Ondřej Caletka

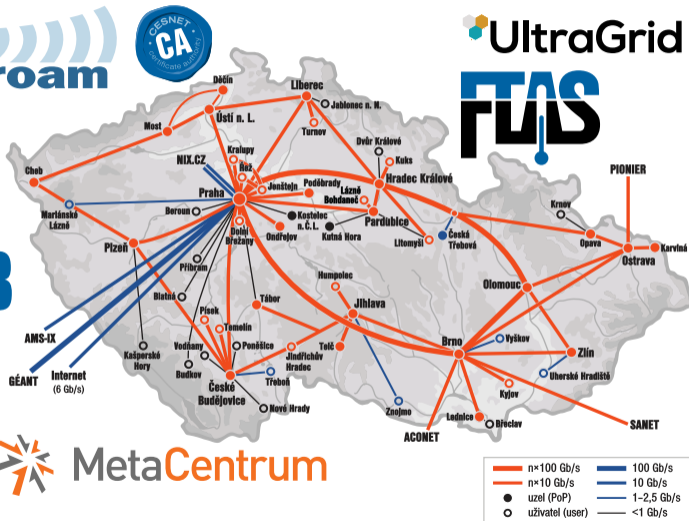


12. listopadu 2015

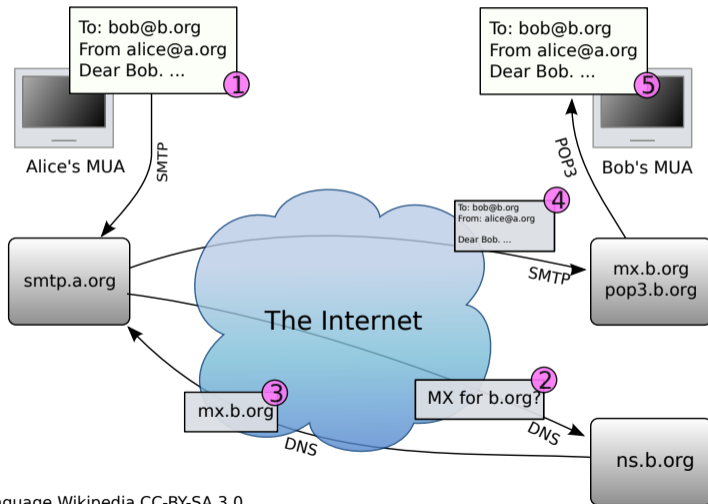


Uvedené dílo podléhá licenci Creative Commons Uveďte autora 3.0 Česko.

O sdružení CESNET



Princip SMTP



Kdo poslouchá?

- server odesílatele
- server příjemce
- **kdokoli s odbočkou na kabelu**

Best Current Practice #188

Internet Engineering Task Force (IETF)
Request for Comments: 7258
BCP: 188
Category: Best Current Practice
ISSN: 2070-1721

S. Farrell
Trinity College Dublin
H. Tschofenig
ARM Ltd.
May 2014

Pervasive Monitoring Is an Attack

Abstract

Pervasive monitoring is a technical attack that should be mitigated in the design of IETF protocols, where possible.

End-to-end

- S/MIME – CMS
- PGP
- ✓ vysoká úroveň bezpečnosti
- ✗ obtížné použití uživatelem

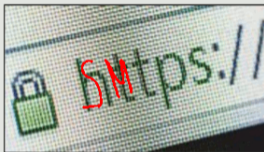
Hop-by-hop

- DKIM
- **SMTP over TLS**
- ✓ bez přímé účasti uživatele
- ✗ jen proti třetím stranám

Oportunistické šifrování

- server signalizuje podporu STARTTLS
- klient naváže anonymní TLS spojení
 - ověření identity se neprovádí
 - vyhoví i slabé a nebezpečné šifry
- při selhání TLS spojení je **doručeno bez šifrování**
- odolné pouze proti pasivnímu odposlechu
- lze definovat cíle s vynuceným šifrováním
 - např. Gmail, Seznam,...
 - jak takový seznam získat a udržovat?

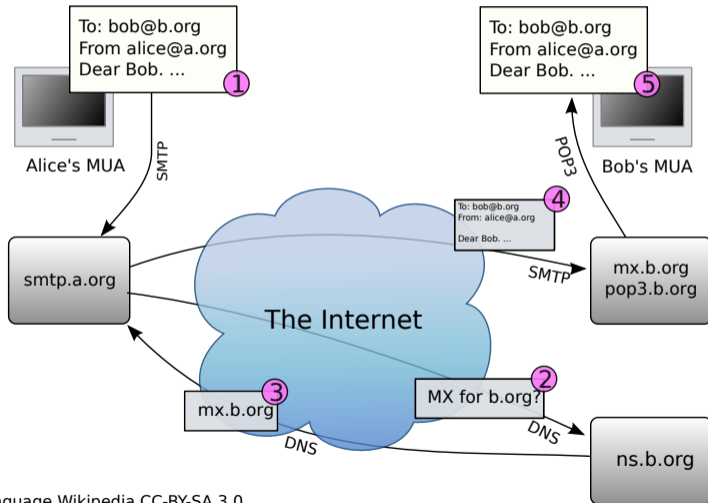
~~SM~~TPS BY MĚLO BÝT VŠUDE



Celý internet směřuje k šifrování. Bezpečnostních kauz přibývá a s nimi se násobí úsilí rozšířit i šifrování mezi uživatelem a službami. ~~SM~~TPS by se mělo stát standardem, který bude nejen očekáván, ale i vyžadován na mnoha úrovních: od prohlížečů až po uživatele. Výsledkem bude lepší ~~web~~ ^{E-MAIL} pro všechny.

- všechny SMTP servery přijímají poštu šifrovaně
- každý SMTP server používá validní TLS certifikát od důvěryhodné authority
- předávání e-mailů je pak naprosto bezpečné
...nebo snad ne?

Princip SMTP



Ten DNSSEC bude asi fakt potřeba...

- bez bezpečného DNS není možné věřit směrování MX záznamů
- certifikáty serverů by musely být vystaveny na jméno domény, pro kterou přijímají poštu
 - což je stejně špatné, jako u dnešního webu
 - pro e-mailů velmi nepraktické
- bezpečné DNS může nést informaci o vynucení šifrování předávané pošty

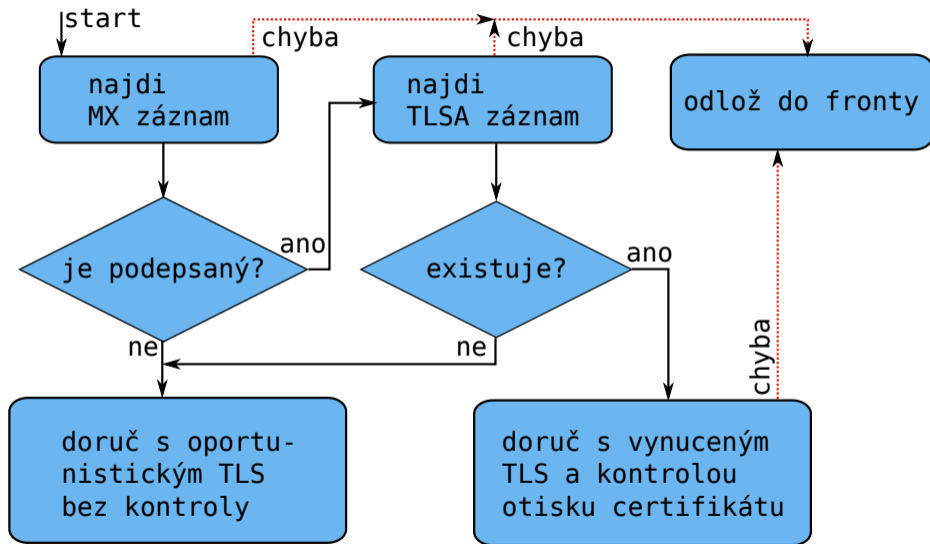
TLSA záznam pro vynucení šifrování

- umístění otisku serverového certifikátu v DNS
- použití pro SMTPS standardizováno v RFC 7672
- několik různých způsobů použití:
 - 0 připíchnutí CA
 - 1 připíchnutí koncového certifikátu
 - 2 vložení nové CA
 - 3 vložení koncového certifikátu bez ohledu na PKI

Příklad

```
_25._tcp.mx.example.com. IN TLSA 3 1 1 AA793DA...
```

Chování SMTP klienta



Opt-in for security

- umístěním TLSA záznamu deklaruujeme, že poštu přijímáme pouze šifrovaně
- validující klienti případný *downgrade* útok odhalí a zprávu nedoručí
 - Postfix od 2.11
 - Exim - ve vývoji
 - OpenSMTPd - ve vývoji
- na rozdíl od webu na SMTP serverech není problém s funkcí DNSSEC validace
- bezpečné spojení s validujícím DNS serverem **je nutné** (ideálně Unbound na localhost)
- doručování na adresy bez DNSSECu nebo bez TLSA záznamu funguje jako doposud



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)
```

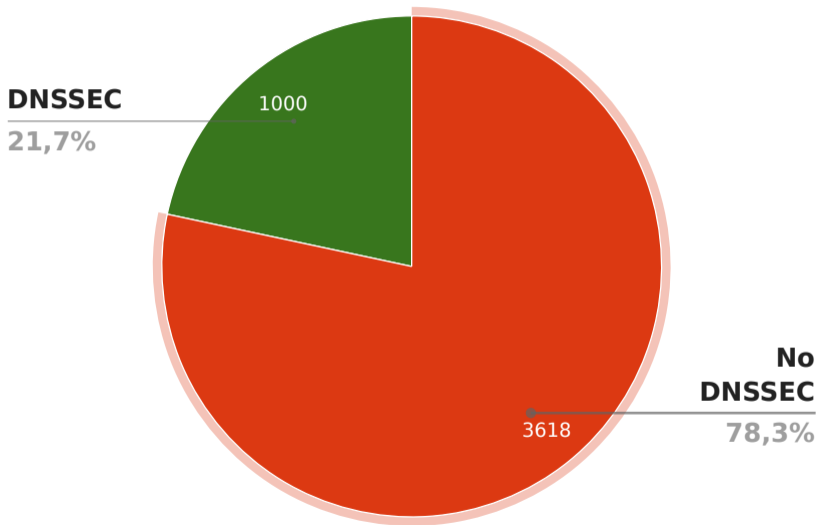
S TLSA záznamem – Verified

```
$ /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)
```

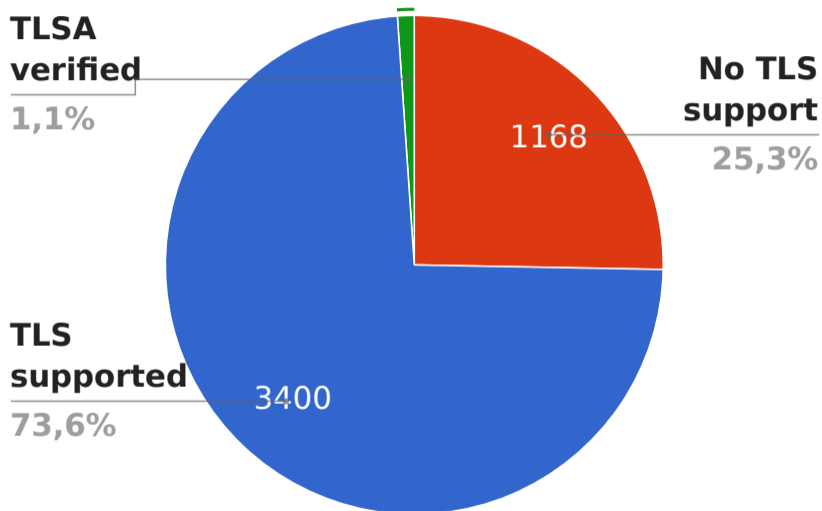
Měření SMTP-over-TLS

na 4618 doménových jménech z reálného provozu

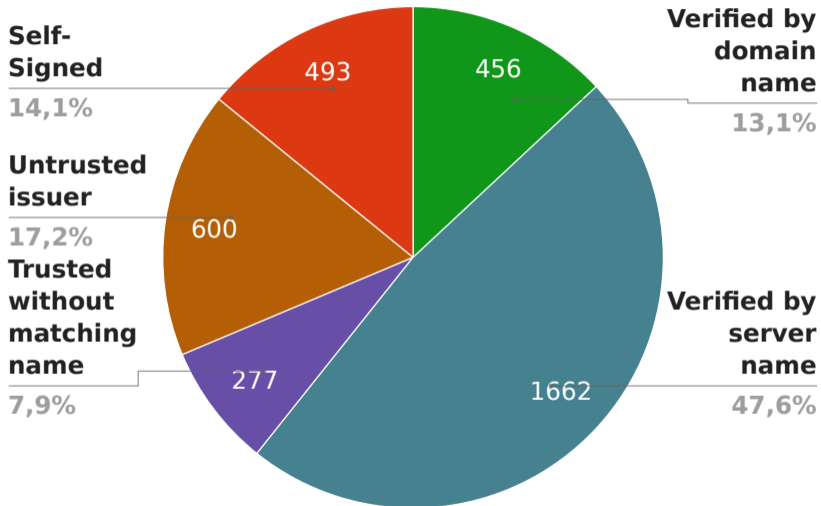
Stav DNSSEC pro MX záznamy



Severy podporující STARTTLS



Typy certifikátů na SMTP serverech



TLSA Hall of Fame

hostel.eduid.cz doesnotwork.eu
lrz.uni-muenchen.de
listen.jpberlin.de
csirt.cz elixir-czech.cz
oskarcz.net caletka.cz zkb.csirt.cz
debian.org isc.org nic.cz
linuxdays.cz tuhh.de eduroam.cz
jirit.cz switch.ch www.cesnet.cz
nebezi.cz ces.net gitima.eu cesnet-ca.cz
rt.cesnet.cz jesenickymaraton.cz
rt4.cesnet.cz tum.de rub.de restena.lu
roboot.cz mzk.cz tu-harburg.de gacr.cz
projects.cesnet.cz gitima.cz
lrz.de
eduid.cz monstersu.cesnet.cz
vspj.cz belnet.be stech.cz
lists.nic.cz rt3.cesnet.cz turris.cz
rcna.cesnet.cz ietf.org chemie.uni-kl.de
valasskyhrb.cz cesnet.cz unitymedia.de

WordItOut



- povolte šifrování na svých SMTP serverech
 - nic to nestojí
 - na typu certifikátu vůbec nezáleží
- bez DNSSECu nelze dosáhnout bezpečnosti e-mailu
- když už máte DNSSEC, TLSA nic nestojí
- provozovat validaci je bezpečné
 - ale vyplatí se sledovat logy na výskyt chyby
Server certificate not trusted

Děkuji za pozornost

Ondřej Caletka

Ondrej.Caletka@cesnet.cz

<https://Ondrej.Caletka.cz>

