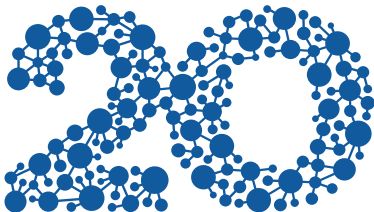


Bezpečnější pošta díky DANE

Ondřej Caletka



1996–2016

CESNET

SPOLUPRÁCE
VÝZKUM
KOMUNITA

2. dubna 2016



Uvedené dílo podléhá licenci Creative Commons Uvedte autora 3.0 Česko.

O sdružení CESNET

edu ID cz

eduroam



CESNET
CMRTS

Mentat



Warden

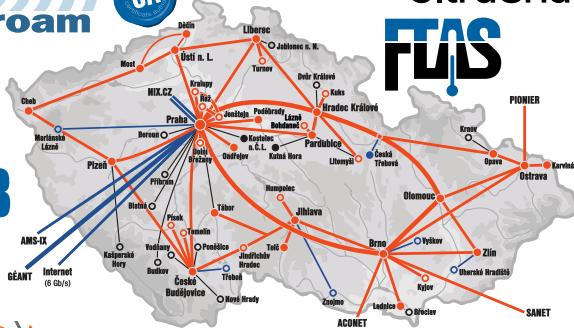
CESNET
DataCare

MetaCentrum

UltraGrid

FUS

PIONIER



— (thick orange)	n×100 Gb/s	— (thick blue)	100 Gb/s
— (medium orange)	n×10 Gb/s	— (medium blue)	10 Gb/s
— (thin orange)	1-2,5 Gb/s	— (thin blue)	1-2,5 Gb/s
● (black)	uzel (PoP)	○ (white)	<1 Gb/s
○ (white)	uživatel (user)	— (grey)	<1 Gb/s



1996–2016
CESNET

Elektronická pošta

- starší než Internet
- přepojování zpráv *ulož a předej*
- na internetu používá protokol SMTP

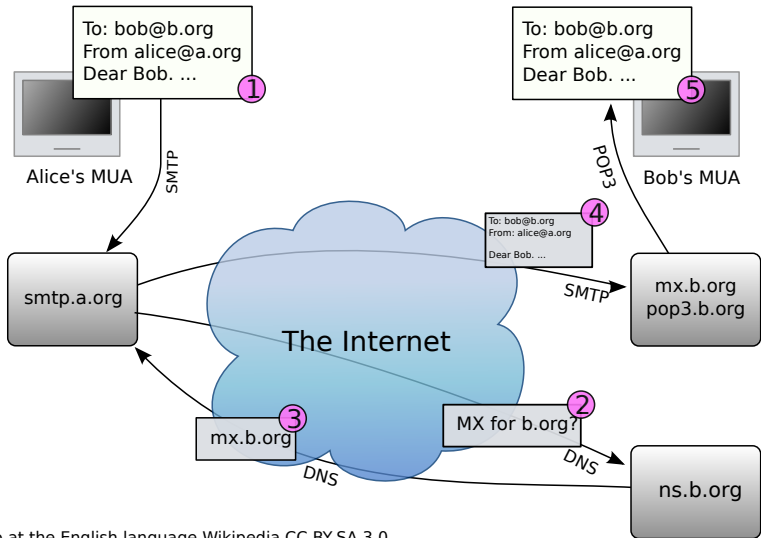
E-mailová etiketa

E-mail není důvěrný: Do e-mailu nepište nic, co byste nenapsali na zadní stranu pohlednice. Vaše e-mailová korespondence se kdykoli může dostat do nepovolaných rukou... zdroj



1996-2016
CESNET

Princip SMTP



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



1996-2016
CESNET

Kdo poslouchá?

- server(-y) odesílatele
- server(-y) 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

Hop-by-hop

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



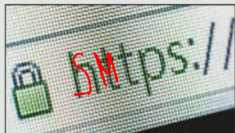
Oportunistické šifrování

- 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?



V ideálním světě...

~~SM~~TPS BY MĚLO BÝT VŠUDE



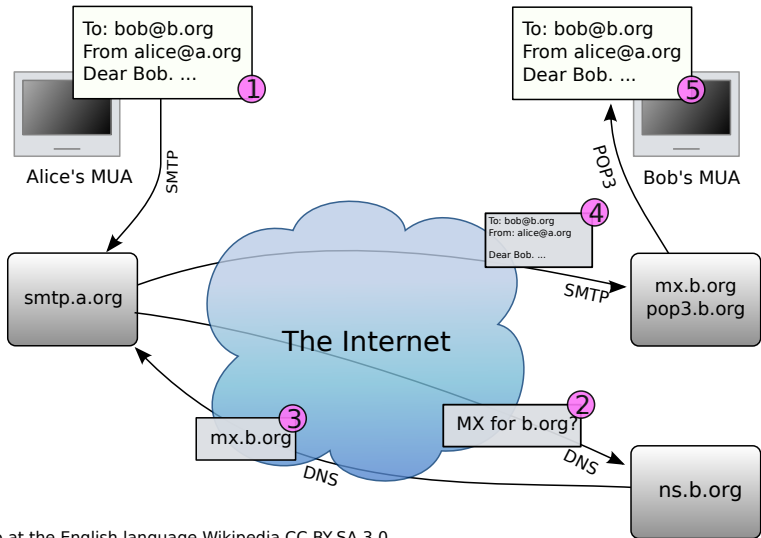
Celý internet směřuje k šifrování. Bezpečnostních kauz přibývá a s nimi se násobí úsilí rozšířit i šifrování mezi uživatelem a službami. ~~SM~~TPS by se mělo stát standardem, který bude nejen očekáván, ale i vyžadován na mnoha úrovních: od prohlížečů až po uživatele. Výsledkem bude lepší ~~web~~ ^{E-MAIL}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

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



1996–2016
CESNET

Princip SMTP



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



1996-2016
CESNET

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-maily velmi nepraktické
 - protože to nemají všichni, nelze to vynutit
- 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

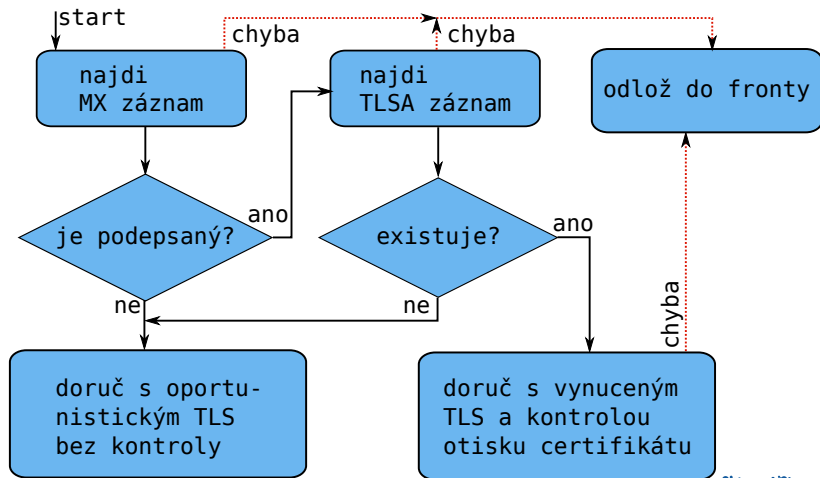
Příklad

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



1996–2016
CESNET

Chování SMTP klienta



1996–2016
CESNET

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 funkčností 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)
```



1996–2016
CESNET

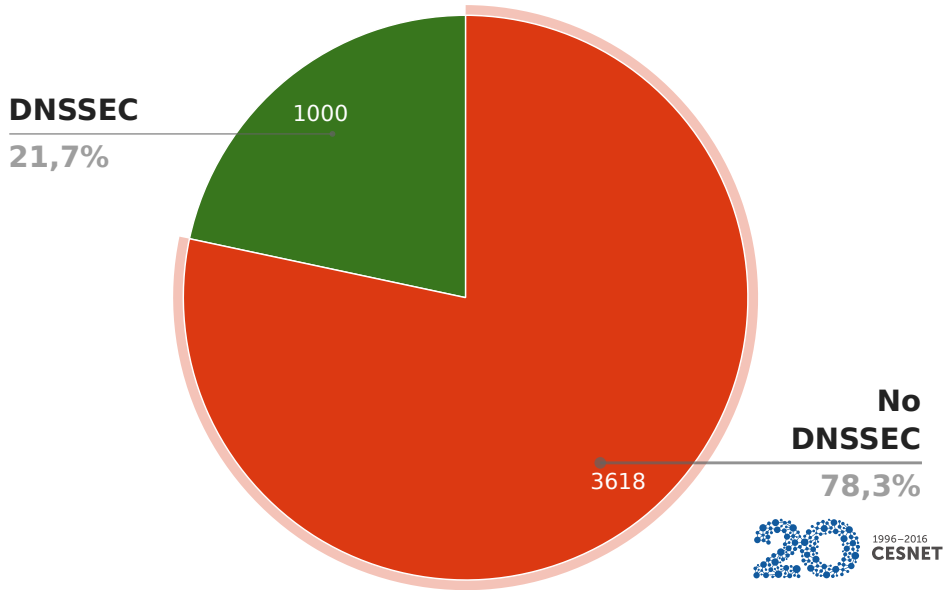
Měření SMTP-over-TLS

na 4618 doménových jménech z reálného provozu



1996–2016
CESNET

Stav DNSSEC pro MX záznamy



Servery podporující STARTTLS

**TLSA
verified**

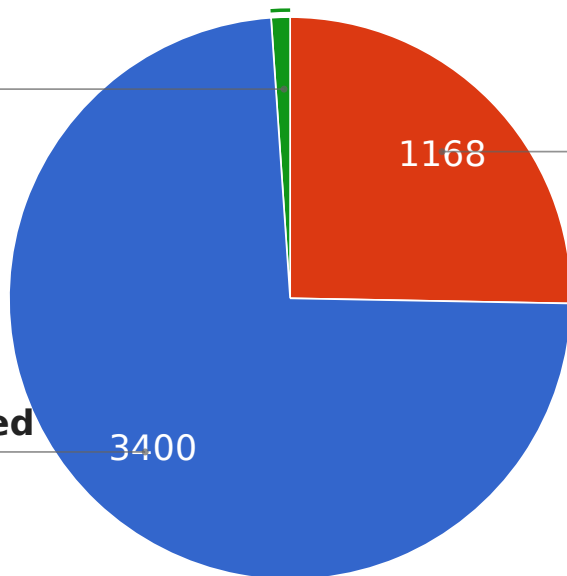
1,1%

**No TLS
support**

25,3%

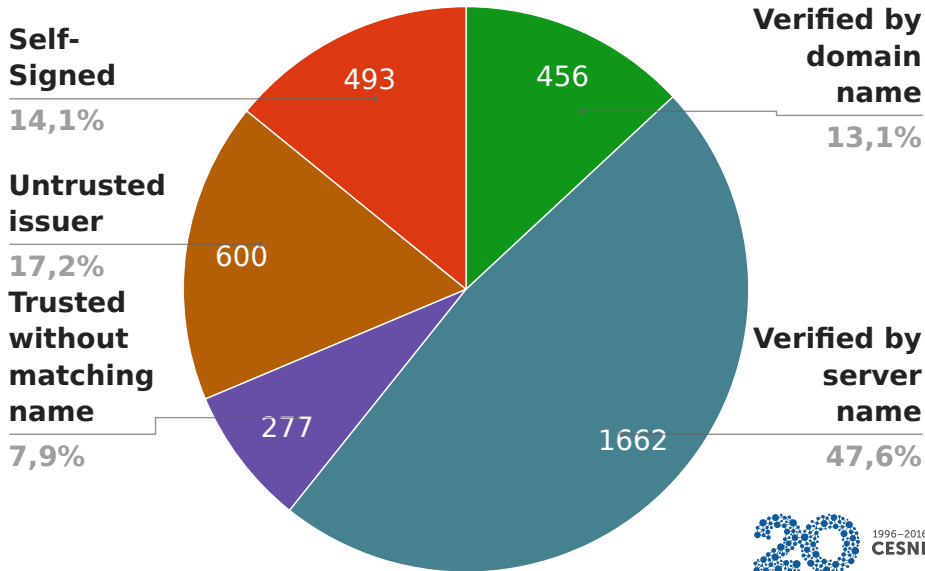
**TLS
supported**

73,6%



1996-2016
CESNET

Typy certifikátů na SMTP serverech



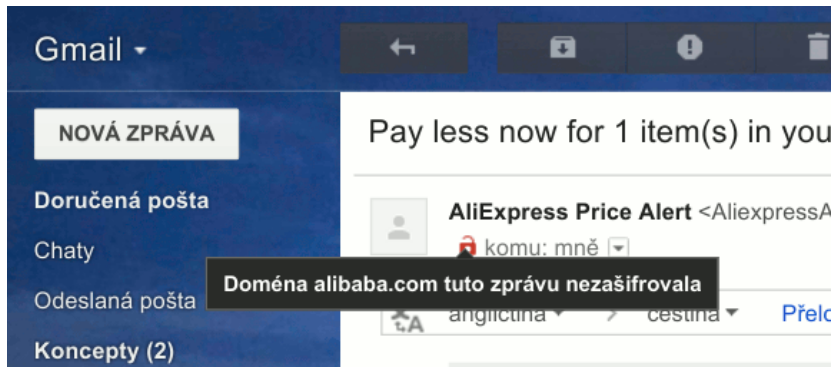
1996–2016
CESNET

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
robot.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



Upozornění Gmailu na zprávu přijatou bez šifrování



The screenshot shows the Gmail interface. On the left is a dark blue sidebar with the 'Gmail' logo and navigation options: 'NOVÁ ZPRÁVA', 'Doručená pošta', 'Chaty', 'Odeslaná pošta', and 'Koncepty (2)'. The main area shows an email header with the subject 'Pay less now for 1 item(s) in you' and the sender 'AliExpress Price Alert <AliexpressA...>'. Below the sender name, there is a red padlock icon and the text 'komu: mně'. A black warning box is overlaid on the email content, containing the text: 'Doména alibaba.com tuto zprávu nezašifrovala'. At the bottom of the email header, there are language selection options for 'angličtina' and 'čeština', and a 'Přelož' link.



1996–2016
CESNET

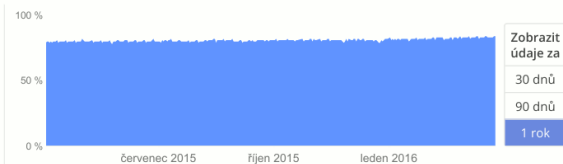
Statistiky STARTTLS u Gmailu

Odchozí



84 %

Zprávy z Gmailu
jiným
poskytovatelům.

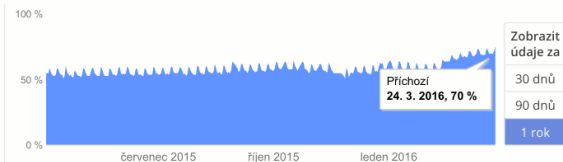


Příchozí



75 %

Zprávy od jiných
poskytovatelů
do Gmailu.



Zdroj: Google Transparency Report



1996–2016
CESNET

- 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

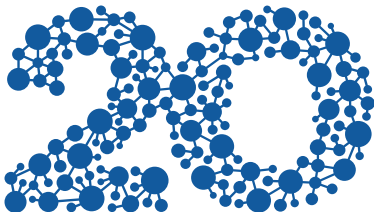


Děkuji za pozornost

Ondřej Caletka

Ondrej.Caletka@cesnet.cz

<https://Ondrej.Caletka.cz>



1996–2016

CESNET

SPOLUPRÁCE
VÝZKUM
KOMUNITA