

E-mailové reputační systémy

Ondřej Caletka

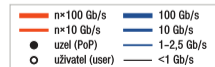


18. júna 2017



Uvedené dílo podléhá licenci Creative Commons Uvedte autora 3.0 Česko.

O sdružení CESNET



MetaCentrum



UltraGrid

- 1 Stručně o elektronické poště
- 2 Sender Policy Framework
- 3 DomainKey Identified Mail
- 4 Author Domain Signing Practices
- 5 Domain-based Message Authentication, Reporting, and Conformance
- 6 Authenticated Received Chain

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:

- 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

```
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
```

Sender Policy Framework

- původně *Sender Permitted From*
- nasazeno před standardizací
- váže identitu odesílatele s DNS záznamem
- cílem je zabránit falšování identity odesílatele
- majitel domény specifikuje, které servery jsou oprávněny jeho jménem posílat poštu

Příklad SPF politiky

```
example.com. IN TXT "v=spf1 ip4:192.0.2.0/24 -all"
```

Přehled kvalifikátorů

- + *pass* - vyhovuje - výchozí
- ? *neutral* - neznámý
- *fail* - nevyhovuje
- ~ *softfail* - spíše nevyhovuje

- server validuje v průběhu SMTP komunikace IP adresu serveru
- nejprve s doménou příkazu HELO/EHLO
- poté s doménou z MAIL FROM:
- podle výsledku analýzy *se nejspíš něco stane*:
 - pass zpráva je propuštěna
 - neutral zpráva je přezkoumána antispamem
 - fail zpráva je odmítnuta při SMTP komunikaci
 - softfail zpráva je podrobena důkladnějšímu zkoumání/přesunuta do karantény
- SPF nechává volnost ve využití výsledků analýzy

- původně vyvinuto se záznamem typu TXT
 - *zneužití* generického typu
- později standardizován záznam typu SPF
- obtížný přechod, validátory musely načítat oba typy
- RFC 7208 použití záznamu typu SPF rezervuje pro budoucí verze SPF

Problém s přeposíláním pošty

Problematické chování

- A publikuje SPF ve stylu ip4:... -all
- B umožňuje přeposílání došlé pošty
- C validuje SPF a při *fail* zprávy odmítá

A posílá poštu do B, ta je následně přeposlána do C
C vidí poštu od A doručenou z IP adresy serveru B

Možná řešení

- A použije *softfail*
- B přepíše zpáteční adresu
- C vyhodnotí *fail* stejně jako *softfail*

T

- na prázdnou adresu <>
 - odesílatel se nedozví případné problémy s doručením přeposlané zprávy
- na adresu administrátora
 - problémy se dozví administrátor
- na speciální adresu, která je přeposílaná na původní
 - většinou nejlepší řešení
 - nesmíme při tom vytvořit *open relay*

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

- nejstarší pokus o autentizaci odesílatele
- řeší jen obálkové adresy
- nedefinuje chování příjemce zprávy
- přeposílání *broken by design*

Pokud máte rádi své uživatele...

- nepoužívejte *hard fail* politiku
- neodmítejte poštu s výsledkem *hard fail*
- implementujte SRS, zvláště pokud přeposíláte

DomainKey Identified Mail

- zvýšení autenticity elektronických zpráv
- použití elektronického podpisu (resp. značky)
- podepisování na serveru
- podpis jako přídatná hlavička
- veřejný klíč uložený v DNS
- kdokoli může podepisovat i validovat
- zprávy s nevalidním podpisem nemají být diskriminovány proti zprávám bez podpisu

Příklad DKIM podpisu

```
DKIM-Signature: v=1; a=rsa-sha256; d=example.com;  
bh=3yZ...h2=; c=relaxed/relaxed; s=dep1;  
h=Date:From:To:Subject:From; b=Wo/qoyff...M0yBh5UqQ=
```

v= verze DKIM

a= algoritmus podpisu

d= doména podpisu

bh= hash těla zprávy

c= kanonizace hlaviček/těla

s= DNS selektor

h= seznam podepsaných hlaviček

b= vlastní podpis

Příklad DKIM klíče

```
dep1._domainkey.example.com. IN TXT "v=DKIM1; k=rsa;  
p=MIIBIjANBgkqhkiG9w0BAQE... " " ...U9W"
```

- TXT záznam v subdoméně `_domainkey`
- veřejný klíč v Base64 ☹
- uvozen selektorem - libovolný řetězec
 - plynulá výměna klíčů
 - různé klíče pro různá oddělení
- limit 255 znaků na jeden *label* v TXT záznamu
 - problém s velkými RSA klíči
 - stačí složit záznam z více kratších *labelů*

Kanonizace

- předúprava zpráv před podepisováním
- cílem je zachovat podpis, pokud někdo po cestě *pokazí* zprávu
 - změna velikosti písmen v hlavičkách
 - přeformátování bílých mezer v těle zprávy
- nastavení `simple` úpravu neprovádí
- nastavení `relaxed` je imunní vůči nevýznamným úpravám

Příklad DKIM podpisu

```
DKIM-Signature: v=1; a=rsa-sha256; d=example.com;  
bh=3yZ...h2=; c=relaxed/relaxed; s=dep1;  
h=Date:From:To:Subject:From; b=Wo/qoyff...M0yBh5UqQ=
```

↑

Podepisování hlaviček

- podepsány jsou jen ty, které jsou vyjmenovány v podpisu + samotný podpis
- vícenásobný výskyt v podpisové hlavičce znamená vícenásobný počet hlaviček
- důležité hlavičky je možné *přepodepsat* (oversign)

Příklad DKIM podpisu

```
DKIM-Signature: v=1; a=rsa-sha256; d=example.com;  
bh=3yZ...h2=; c=relaxed/relaxed; s=dep1;  
h>Date:From:To:Subject:From; b=Wo/qoyff...M0yBh5UqQ=
```

- snaha deklarovat, že daná doména podepisuje své zprávy
- možnost zahazovat prokazatelně zfalšované zprávy (např. PayPal)
- jednoduchá deklarace pomocí TXT záznamu v subdoméně `_adsp._domainkey`
- neúspěch - v roce 2013 prohlášeno za historický standard

Příklad ADSP deklarace

```
_adsp._domainkey.example.com IN TXT "dkim=all"
```

Možné politiky

unknown neexistující (výchozí)

all všechny zprávy by měly být podepsány

discardable nesprávně podepsané zprávy mají být zahozeny (není určeno pro lidi)

Problém s e-mailovými konferencemi

- konference často upravují zprávy
 - odstraňují nevhodné přílohy
 - přidávají tagy do předmětu
 - přidávají patičky
- přitom je žádoucí zachovat identitu původního odesílatele
- konference by měla přepodepisovat
- konference by neměla přijímat respondenty s ADSP discardable
- konference může **měnit adresu From:**
 - jediné funkční řešení
 - znemožňuje automatické ověření PGP a S/MIME podpisů

Domain-based Message Authentication, Reporting, and Conformance

- systém ověření identity odesílatele (hlavičky From:)
- používá výsledky analýzy SPF a DKIM
- přesně definované nakládání se zprávou, která nevyhoví
- automatizované hlášení problematických zpráv
- možnost postupného nasazení

Příklad DMARC záznamu

```
_dmarc.example.com IN TXT "v=DMARC1; p=none"
```

Význam voleb

v= verze

p= politika (none, quarantine, reject)

pct= procento zpráv, které bude kontrolováno

adkim= asociace DKIM k odesílatelově doméně

aspf= asociace SPF k odesílatelově doméně

rua= reportování agregovaných statistik

ruf= reportování zpráv, kde selhalo ověření

Hlášení o problémech

- agregované statistiky jednou za den a okamžité reporty nevyhovujících zpráv
 - většina provozovatelů podporuje jen agregované statistiky
- doručení e-mailem v zazipovaném XML souboru
- limit na velikost zprávy
- reportování do cizích domén nutno autorizovat v DNS

Příklad reportování z A.org do B.org

```
... IN TXT "...rua=mailto:dmarc-rua@B.org!10m"  
A.org._report._dmarc.B.org. IN TXT "v=DMARC1"
```

Problém 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

Authenticated Received Chain

- IETF draft řešící problém DMARC s e-mailovými konferencemi
- vychází z DKIM
- podepisuje směrovací hlavičky Received:
- poskytne důkaz, že zpráva byla před vstupem do konference řádně podepsaná
- poskytne důkaz, kdo danou zprávu upravoval
- pozitivní ověření ARC zabrání odmítnutí předané zprávy podle DMARC

- hygiena správného užívání e-mailových schránek
 - příjem pošty protokoly IMAP/TLS, případně IMAPS
 - předávání pošty k odeslání autentizovaným protokolem Submission/TLS, případně SMTPS
 - **žádné přeposílání přes *open relay* místního ISP**
- SPF je dobré pro pozitivní určení správného serveru
 - pro ostatní nanejvýš *softfail*
 - pokud nabízíme přeposílání, chce to SRS
- DKIM nikdy neublíží, někdy pomůže
 - není důvod ho nemít
- DMARC má budoucnost
 - velcí hráči už ho mají
 - my ostatní se musíme přizpůsobit
 - ale stále nefunguje s konferencemi

Děkuji za pozornost

Ondřej Caletka

Ondrej.Caletka@cesnet.cz

<https://Ondrej.Caletka.cz>



Prezentace je již nyní k dispozici ke stažení.