Email és DKIM

Kadlecsik József
MTA Wigner Fizikai Kutatóközpont
kadlecsik.jozsef@wigner.mta.hu

Tartalom

- SMTP (ESTMP)
- DKIM
- DMARC
- Tapasztalatok

SMTP I.

Kliens	**Szerver**
<connect>	220 server-fqdn ESMTP xxx
EHLO client-fqdn	250-server-fqdn
	250-PIPELINING
	250 DSN
MAIL FROM: <envelope-from>	250 2.1.0 Ok
RCPT TO: <envelope-to>	250 2.1.5 Ok

SMTP II.

Kliens	**Szerver**
DATA	354 End data with <CR><LF>.<CR><LF>
From: <from>	
To: <to>	
Subject: subject	
Date: date	
body	
.	250 2.0.0 Ok: queued as <queue-id>

A kliens mit hamisíthat?

EHLO client-fqdn

MAIL FROM: <envelope-from>

RCPT TO: <envelope-to>

DATA

From: <from>

To: <to>

Subject: subject

Date: date

body

.

Mi magunk mit hamisítunk?
Forward

EHLO client-fqdn

MAIL FROM: <envelope-from>

RCPT TO: <envelope-to>

DATA

From: <from>

To: <to>

Subject: subject

Date: date

body

.

Mi magunk mit hamisítunk?
Levelezési listák

EHLO client-fqdn

MAIL FROM: <envelope-from>

RCPT TO: <envelope-to>

DATA

From: <from>

To: <to>

Subject: subject

Date: date

body

.

Email hitelesítési lehetőségek

- Mail User Agent (MUA): digitális aláírás
  - PGP
  - X.509
- Mail Transport Agent (MTA):
  - SPF
  - DKIM

SPF

- SPF: Sender Policy Framework
  - SMTP before queue szűrés
  - Mely SMTP szerver küldhet @domain alakú feladóval emailt
    - Envelope, Mail From:
    - DNS TXT record
- False positive (naivul)
  - Forward

DKIM

- DKIM: DomainKeys Identified Mail
  - SMTP after queue szűrés
  - DKIM-Signature fejléc, benne digitális hash:
    - Aláírt fejlécek
    - Message body
  - DNS TXT record
- False positive (naivul)
  - Levelezési listák

DNS TXT record

- `20151130._domainkey.wigner.mta.hu. 14400 IN TXT "v=DKIM1; k=rsa; t=s; p=..."`
- Selector
  - Tetszőleges, tipikusan YYYYMMDD
- t=y:s
  - y: teszt mód
  - s: subdomainre is érvényes

DKIM-Signature fejléc

```
DKIM-Signature: v=1; a=rsa-sha256;
c=relaxed/relaxed; d=wigner.mta.hu;
h=mime-version:user-
agent:references:message-id:in-reply-to
:from:from:date:date:received:received:rec
eived:received; s=20151130; t=1457883089;
x=1459697490;
bh=j2e9uzF+s/6GFmD7tMPBt+euSO00ED90w1DtcZV
4qzM=;
b=lVfBi+HWrvtH+ttd70HFeK6tswYzrER4DAes/Mi
```

Kinek a leveleit írjuk alá?

- Belső (megbízható) hálózat kliensei
- Belső hálózaton levő levelezési lista szerver
- Külső kliensek SASL autentikáció után

DKIM és levelezési listák

- Módosíthatják a Subject: fejlécet
  - Kizárható az aláírt fejlécek közül
- Módosíthatják a levél törzsét (header, footer)
  - l=0 megadható lenne a body hash számításához, de
    - Amavisd-new + Spamassassin/Mail::DKIM
      - Ignorálja az „l” paramétert aláíráskor, azaz az egész body-t aláírja
      - Ignorálja a hash ellenőrzésekor, azaz az egész body-t ellenőrzi
  - Body hash ellenőrzése kihagyható Spamassassin-ban
    - Minimális patch

DMARC I.

- Domain-based Message Authentication, Reporting and Conformance
- DKIM és SPF működéséhez, a fogadó oldalon
  - Milyen mechanizmust használ a küldő: aspf, adkim
  - Milyen ellenőrzést vár el a megadott(ak)ra: s(strict), r(relaxed)
  - Hogyan kezelje a fogadó a nem valid leveleket, azaz policy: none, quarantine, reject
  - A levelek hány százalékára: pct
  - A küldő kér-e és ha igen, hova aggregált és/vagy részletes failure reportot: rua, ruf

DMARC II.

```
_dmarc.wigner.mta.hu. 1800  IN  TXT
"v=DMARC1; p=none; adkim=s; pct=100;
rua=mailto:dmarc-report@wigner.mta.hu;
ruf=mailto:dmarc-report@wigner.mta.hu"
```

DKIM hol nem működik megbízhatóan

- Levelezési listák
  - Subject-et nem írjuk alá
  - Body hash-t nem ellenőrizzük
- Felhasználók külső levelező szervert/gmail-t használ
  - Figyelmeztetjük őket
  - Lassú folyamat
  - …vagy beállítja a gmail-ben a mi szerverünket levélküldésre…

Hol nem működik, folyt.

- Majordomo nem default purge_received = yes
  - khronos.org: report küldés, kijavították
- Proxy tűzfal (alf) törölheti a Received sorokat
- googlegroups.com (postmaster@google.com):
  - DKIM-Signature fejlécet törlik
    - From:-ot átírják, ha DMARC policy nem 'none'
  - Kölcsönös hibajavítások:
    - Google: X-Spam-Checked-In-Group
    - Mi: Message-ID

Message-ID

- Outlook 12.0 érvénytelen Message-ID-et generál

```
# /etc/postfix/main.cf
header_checks = pcre:/etc/postfix/hdr_check_pcre
# /etc/postfix/hdr_check_pcre
/^Message-id: (.+)(@)(.+@wigner.mta.hu.+)/
        REPLACE Message-ID: $1.$3
```

Külső web felületek

- Reply-To kellene From helyett…
- Kontakt cím megtalálása kihívás…
- Változó sikerek

Összefoglalás

- Email hamisítás elleni védelem
  - DKIM + DMARC
  - Nem a MUA/MTA okozza a gondot
  - Google „elvárja”