dohnal@openalt:~/email-security $ ./init_deck.sh

Víte kdo vám píše e-mail?

SPF, DKIM a DMARC – Základy bezpečné komunikace

STATUS: OpenAlt | CLEARANCE: Konference | VER: 08.11.2026

Autor:

Ing. Ondřej Dohnal

(Deployment Engineer @ GINA Software s.r.o.)

```
$ TL;DR;
```

Hlavní myšlenka

E-mail může úspěšně projít všemi autentizačními kontrolami a přesto pocházet od útočníka.

`head -n 4 ~/mail/fake.eml`

```
MAIL FROM:<ceo@example.com>
RCPT TO:<employee@example.org>
From: CEO <ceo@example.com>
To: Employee <employee@example.org>
...
```

Klíčová rizika

- From ≠ identita
- SPF ≠ důvěryhodný odesílatel
- DKIM ≠ legitimní zpráva
- DMARC ≠ neprůstřelná ochrana

`dig example.com. TXT | grep spf`

```
example.com. 3600 IN TXT "v=spf1 ip4:192.0.2.0/24 -all"
```

$ Obsah

bat agenda.toml

[01] **Jak opravdu vypadá e-mail?**
SMTP envelope, hlavičky, MAIL FROM, From, Reply-To.

[02] **Sender Policy Framework – *SPF***
Jak funguje, co ověřuje, co neověřuje a jak lze zneužít k útoku.

[03] **DomainKeys Identified Mail – *DKIM***
Kryptografický podpis a jeho omezení.

[04] **Domain-based Message Authentication, Reporting and Conformance**
Alignment, politiky a vyhodnocení.

[05] **Praktická ukázka**
Podvržený e-mail a výsledky autentizace.

[06] **Obrana a závěr**
Správná konfigurace, monitoring, doporučení.

```
$ Víte, kdo vám právě napsal?
```

Nová zpráva

Od: **Fakturační oddělení** <fakturace@example.com>

Předmět: **Neuhrazená faktura – poslední výzva**

Dobrý den,
v příloze zasíláme upomínku k neuhrazené faktuře.
Prosíme o kontrolu a úhradu.

```
bat ~/mail/faktura.eml
MAIL FROM: <bounce@mailer.example>
From: fakturace@example.com
Reply-To: platby@hacker.com
```

Které z těchto adres skutečně důvěřujete?

Ilustrační příklad. Rozdílné adresy samy o sobě neprokazují podvržení.

Sekce 01

Jak opravdu vypadá e-mail?

SMTP envelope, hlavičky, MAIL FROM, From, Reply-To.

$ Jeden e-mail, několik identit

Nová zpráva

Od: **Fakturační oddělení** <fakturace@dodavatel.com>

Předmět: **Neuhrazená faktura – poslední výzva**

Dobrý den,
v příloze zasíláme upomínku k neuhrazené faktuře.
Prosíme o kontrolu a úhradu.

$ SMTP envelope vs hlavičky e-mailu

bat smtp-envelope

```
MAIL FROM: <bounce@mailer.example>
RCPT TO: <uzivatel@example.com>
```

bat email

```
From: fakturace@dodavatel.com
To: uzivatel@example.com
Reply-To: platby@hacker.com
```

Sekce 02

Sender Policy Framework – SPF

Jak funguje, co ověřuje, co neověřuje a jak lze zneužít k útoku.

$ Které servery můžou odesílat poštu za naši doménu?

SPF Verifikace




```
dig example.com. TXT | grep spf
```

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

$ SPF záznam, a jak ho číst

```
dig example.com. TXT
```

```
example.com. IN TXT "v=spf1 ip4:192.0.2.0/24 ip6:2001:db8::1 -all"
```

- `example.com.` – Doména na kterou se dotazujeme
- `v=spf1` – Verze SPF protokolu (1)
- `ip4:192.0.2.0/24` – IPv4 adresy ze kterých je POVOLENÉ posílat e-maily
- `ip6:2001:db8::1` – IPv6 adresy ze kterých je POVOLENÉ posílat e-maily
- `-all` – Způsob zpracování (HardFail – Všechny ostatní IP adresy mají ve SPF selhat)
- `include:spf.example.com` – Přidání záznamů z jiné domény

Pozor!

SPF neověřuje konkrétního člověka ani viditelnou hlavičku `From:`

$ Co SPF neověřuje?

SPF ověřuje server. Ne odesílatele.

SPF ověřuje

- Zdrojovou IP adresu
- Doménu `MAIL FROM`
- Autorizaci v DNS

SPF neověřuje

- Viditelnou hlavičku `From`
- Identitu uživatele
- Obsah zprávy

head report.txt

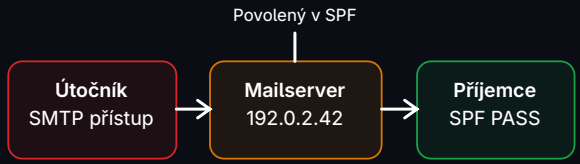
```
MAIL FROM: attacker@evil.example
From: ceo@example.com

SPF: pass - evil.example (192.0.2.154)
```

SPF prošlo, ale nikdo neověřil oprávnění použít `example.com` ve viditelné hlavičce.

$ Útok

Princip útoku



Podmínky útoku

- Přístup k autorizované IP
- Podvržení `MAIL FROM`
- Doména v `MAIL FROM` odpovídá SPF záznamu

$ Kdo najde chybu?

dig chybnezaznamy.example TXT

```
v=spf1 ip4:203.0.113.0/24 ip4:192.0.2.0/24 ip4:198.51.100.0/24
ip6:2001:db8::/32 include:spf.protection.outlook.com -all
```

Sekce 03

DomainKeys Identified Mail

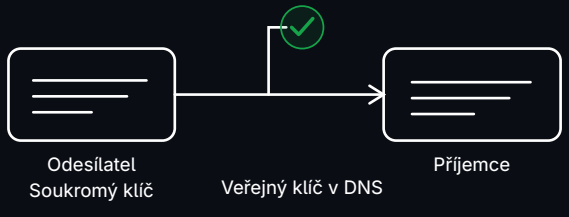
SPF pass. Jsme v bezpečí?
Kryptografický podpis a jeho omezení.

$ Jak ověřit, že e-mail se za doménu nevydává?

tree principle/

> Server podepíše zprávu
> Podpis přidá do `DKIM-Signature`
> Příjemce načte klíč z DNS
> Kryptograficky ověří podpis

Elektronický podpis



$ Náhled pod kapotu

bat dkim.eml

```
DKIM-Signature:
  v=1; a=rsa-sha256;
  d=example.com;
  s=mail2026;
  h=from:to:subject:date;
  bh=...;
  b=...;
```

man dkim

- `v=1` – Verze DKIM
- `a=rsa-sha256` – Použitý algoritmus
- `d=example.com` – Podepisující doména
- `s=mail2026` – selektor
- `h=from:to:subject:date` – Které hlavičky jsou podepsané
- `bh=...` – Hash těla zprávy
- `b=...` – Podpis hlaviček a těla
- ...

DKIM ověřuje podpis domény, nikoliv osobní identitu autora.

$ Ani DKIM není zárukou legitimity

DKIM PASS ≠ důvěryhodná zpráva

Limitace

- Kompromitovaný systém
- Platný podpis, podvodná zpráva
- Jiná podepisující doména
- Neříká, jestli IP může odeslat

bat report.txt

```
From: ceo@example.com

DKIM-Signature:
    d=evil.example;
    s=mail;

dkim=pass
```

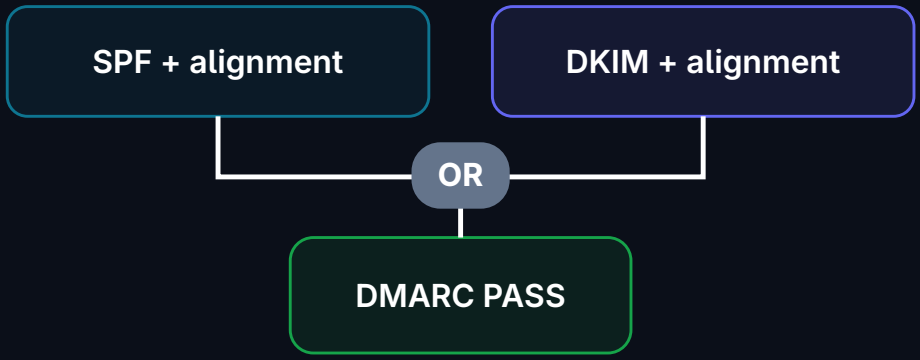
Podpis je platný. Jenže zprávu podepsala jiná doména.

Sekce 04

Domain-based Message Authentication, Reporting and Conformance

Alignment, politiky a vyhodnocení.

$ DMARC propojí výsledky SPF a DKIM s viditelnou doménou



Stačí jedna úspěšná větev

$ DMARC propojí výsledky SPF a DKIM s viditelnou doménou

Alignment (soulad)

From hlavička	Ověřená doména	Režim
example.com	example.com	Strict ✔
example.com	mail.example.com	Relaxed ✔
example.com	evil.example	Neodpovídá ✘

$ DMARC Politiky

dig _dmarc.example.com. TXT

```
_dmarc.example.com. IN TXT
"v=DMARC1; p=reject; rua=mailto:dmarc@example.com"
```

man dmarc

> `v=DMARC1` – Verze DMARC
>
> `rua=...` – Email pro zasílání reportů
>
> `p=...` – Politika
>
> - `reject` – Zamítne vše co neprojde kontrolou
> - `quarantine` – Označí jako podezřelou (SPAM)
> - `none` – Pouze monitoruje, posílá reporty na `rua`
>
> ...

```
$ A teď se vraťme k našemu útočníkovi
```

Útočník využívá povolenou IP adresu a může podvrhnout SMTP envelope.

Odeslaný e-mail

```
MAIL FROM: ceo@example.com
From: ceo@example.com

Sending IP: 192.0.2.42
```

SPF	DKIM	DMARC
PASS	NONE	PASS

Status

Podvržený e-mail prošel DMARC.

$ Proč?

SPF je úspěšné a doména v MAIL FROM odpovídá doméně v hlavičce `From`.
DMARC proto projde i bez DKIM podpisu!

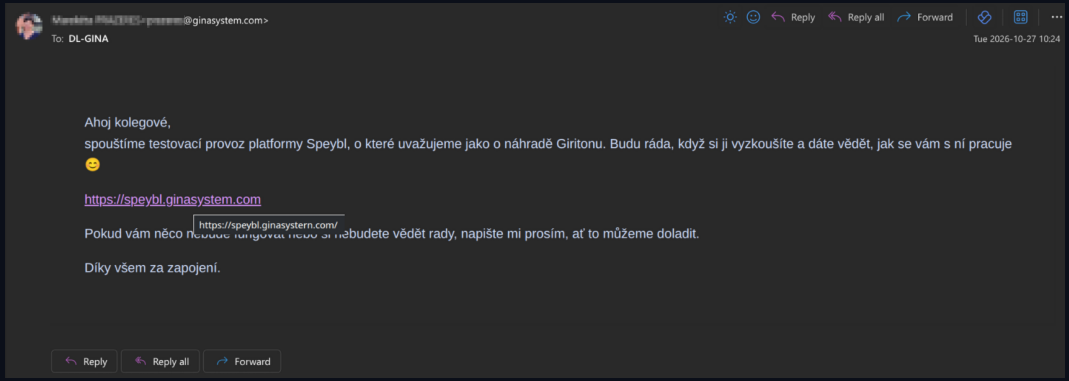
Scénář	SPF	DKIM	DMARC
Neznámá IP, bez podpisu	✗	None	✗
Povolená IP, shodná doména	✓	None	✓
SPF pass pro cizí doménu	✓	None	✗
SPF fail, platné aligned DKIM	✗	✓	✓
SPF pass aligned, DKIM fail	✓	✗	✓

Sekce 05

Praktická ukázka

Podvržený e-mail a výsledky autentizace.

$ Podvodný e-mail



$ Výsledky

Počet osob: 7

Jméno	Uživatelské jméno	Počet pokusů	První výskyt	Poslední výskyt	Detail
[redacted]	[redacted]	15	27. 10. 2026 13:29:45.448 +01:00	27. 10. 2026 13:36:58.063 +01:00	Zobrazit →
[redacted]	[redacted]	1	27. 10. 2026 13:24:12.555 +01:00	27. 10. 2026 13:24:12.555 +01:00	Zobrazit →
[redacted]	[redacted]	1	27. 10. 2026 10:39:11.771 +01:00	27. 10. 2026 10:39:11.771 +01:00	Zobrazit →
[redacted]	[redacted]	3	27. 10. 2026 10:28:20.344 +01:00	27. 10. 2026 10:31:27.003 +01:00	Zobrazit →
[redacted]	[redacted]	4	27. 10. 2026 10:24:29.704 +01:00	27. 10. 2026 10:31:09.334 +01:00	Zobrazit →
[redacted]	[redacted]	3	27. 10. 2026 10:25:30.731 +01:00	27. 10. 2026 10:29:53.121 +01:00	Zobrazit →
[redacted]	[redacted]	1	27. 10. 2026 10:25:27.637 +01:00	27. 10. 2026 10:25:27.637 +01:00	Zobrazit →

Sekce 05

Pár slov závěrem

Co můžu udělat lépe?

$ Na co si dát pozor?

bat /opt/security/checklist.md

- **Příliš široké SPF**: Autorizujeme více infrastruktury, než skutečně potřebujeme
- `+all`: SPF dovoluje libovolnému serveru používat danou doménu
- **Nesprávně delegované odesílání**: Externí služba může posílat zprávy s identitou, kterou nemá používat
- **DNS lookup limity**: SPF skončí `permerror`
- **Chybějící reporting**: Horší kontrola nad skutečným využíváním domény

bat /opt/security/defense.md

- Omezit SPF na skutečně potřebné zdroje
- Podepisovat legitimní odchozí poštu pomocí DKIM
- Používat DMARC s reportingem a vhodně nastavenou politikou
- Auditovat externí poskytovatele a práva k subdoménám
- Monitorovat neobvyklé odesílání a chránit přístupové údaje a podepisovací klíče

$ Závěr - Co si odnést?

SPF – Ověřuje autorizaci serveru k použití domény.

DKIM – Kryptograficky ověřuje podpis domény.

DMARC – Propojuje výsledky autentizace s doménou odesílatele.

Motto

Autentizovaná doména neznamená autentizovaného člověka.

Důvěřujte ověřeným identitám, ale rozumějte tomu, co skutečně ověřujete.

dohnal@openalt:~/email-security $ ./shutdown_presentation.sh -success

DĚKUJI ZA POZORNOST

Otázky & Diskuze

KONTAKT

Email: dohnal@douball.eu

https://github.com/douball3

RFC 7208 - Sender Policy Framework
RFC 6376 - DKIM Signatures
RFC 9989 - DMARC
RFC 8601 - Authentication-Results

Session Terminated Successfully. Press [ESC] to Exit.