

Split Alignment

Diffusing SPF Vulnerabilities with DMARC

Muhammad Hamza¹, Mattijs Jonker², Raffaele Sommese², Simon Fernandez³,
Olivier Hureau³, Eric Pauley^{1,4}, Taejoong Chung¹

¹Virginia Tech • ²University of Twente • ³Univ. Grenoble Alpes • ⁴Terrace Networks



Email Spoofing

4 B+

Active email users:
most used form of
asynchronous
communication. [1]

#1

Phishing/spoofing is
the most reported
cybercrime: 191 K
complaints in 2025. [2]

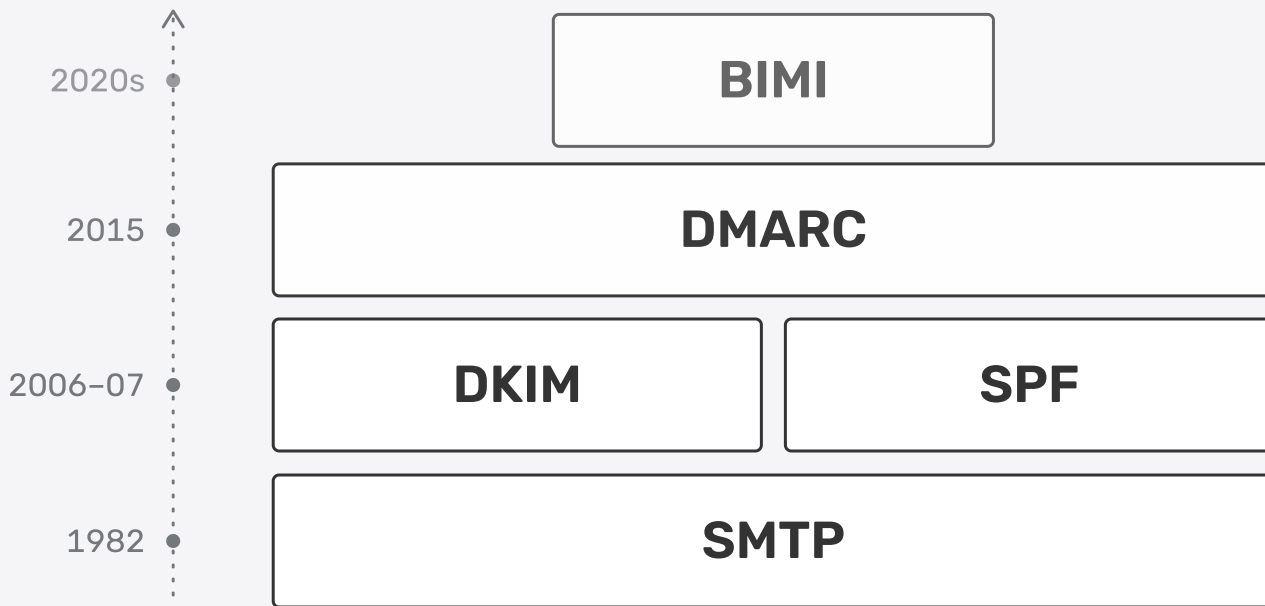
\$216 M

Lost to
phishing/spoofing in
2025. [2]

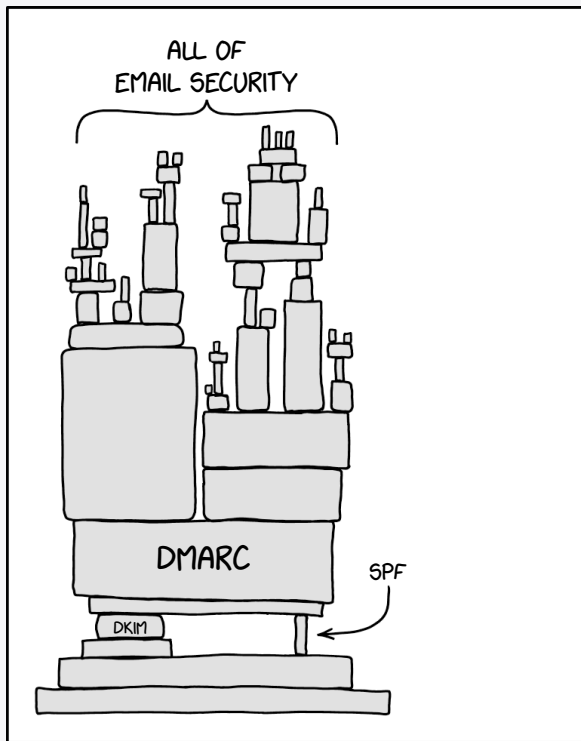
[1] Shopify Staff, "You Should Know These Email Marketing Stats in 2025," Shopify, 2025. shopify.com/blog/email-marketing-statistics

[2] FBI Internet Crime Complaint Center, "2025 Internet Crime Report," 2026. ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

Email Security Stack

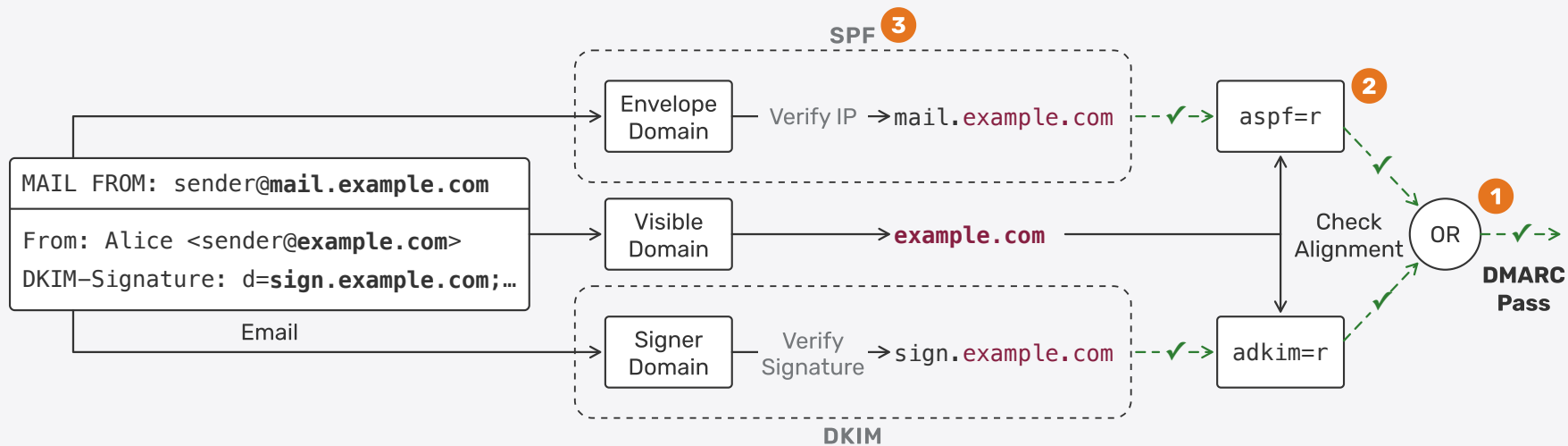


Email Security Stack



xkcd.com/2347 • Randall Munroe (CC BY-NC 2.5), adapted

Email Authentication



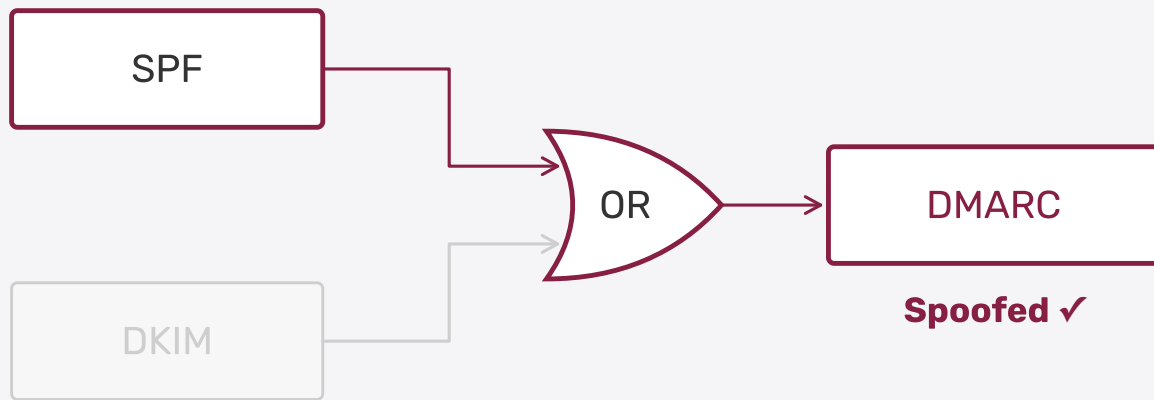
Spoofing Email Using The Weakest Link

OR Clause 1

Relaxed Alignment 2

SPF 3

The weaker of the two can be used to pass DMARC



Spoofing Email Using The Weakest Link

OR Clause 1

Relaxed Alignment 2

SPF 3

Alignment Mode

Authenticated Domain

Visible Domain

Relaxed
=r (default)

mail.example.com

==

example.com

✓ **Aligned**

only org. domain must match

By default, **mail.example.com** can authenticate for any domain in the hierarchy



Spoofing Email Using The Weakest Link

OR Clause ①

Relaxed Alignment ②

SPF ③

bad-spf.example.com. TXT

"v=spf1 ip4:203.0.113.25 ip6:2001:db8::/32 include:spf.thirdparty.com all"

IPs As Security Principals

Core assumptions for IP-based authentication no longer hold because of IP leasing and cloud providers.

Brittle Configuration

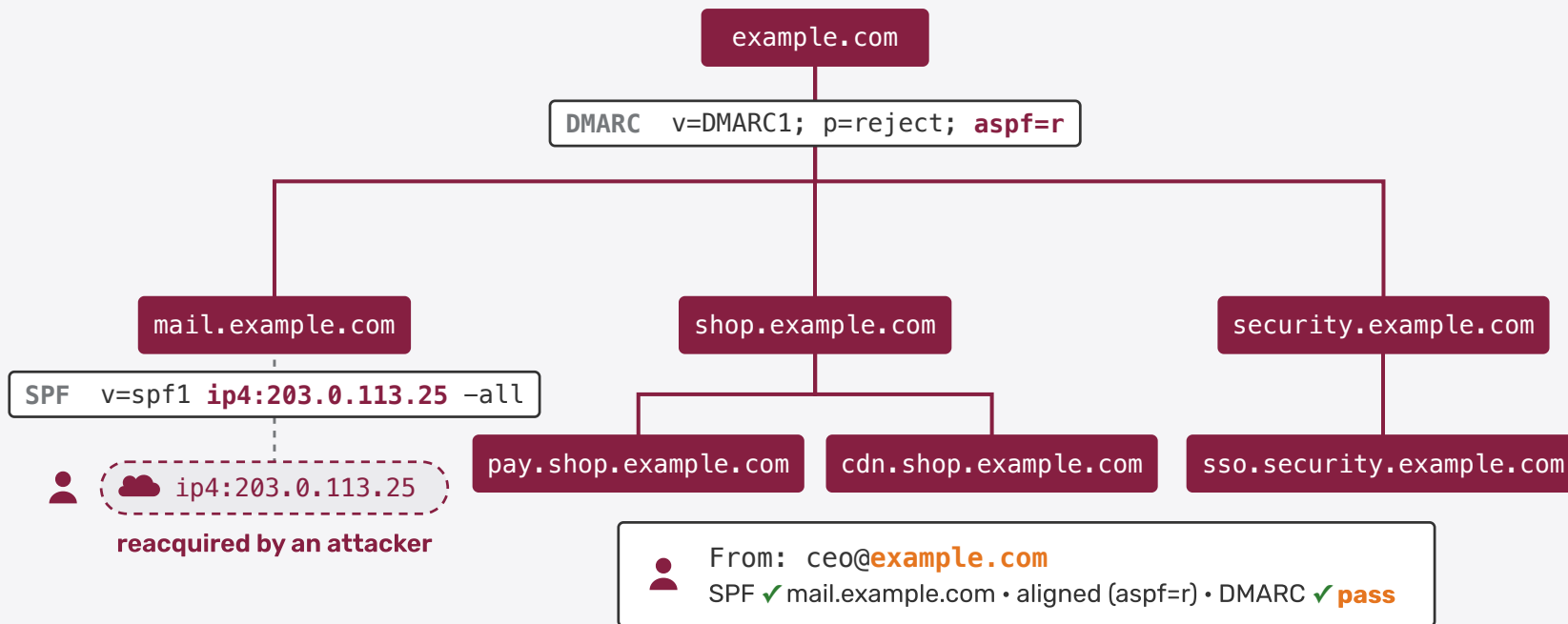
Broad CIDR ranges and chains of includes authorize far more senders than intended.

Permissive By Default

Default qualifier for email disposition is pass, which can lead to unintended consequences from small errors.

Spoofing Email Using The Weakest Link

- OR Clause 1
- Relaxed Alignment 2
- SPF 3



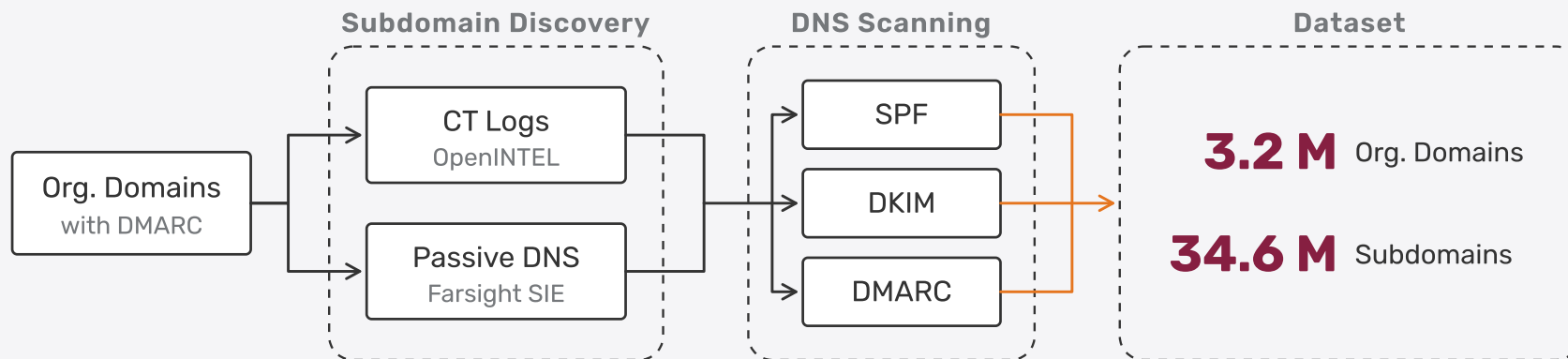
Spoofing In The Wild

Dataset 1

DMARC In The Wild 2

Vulnerable Subdomains 3

DMARC Spoofing 4



Spoofing In The Wild

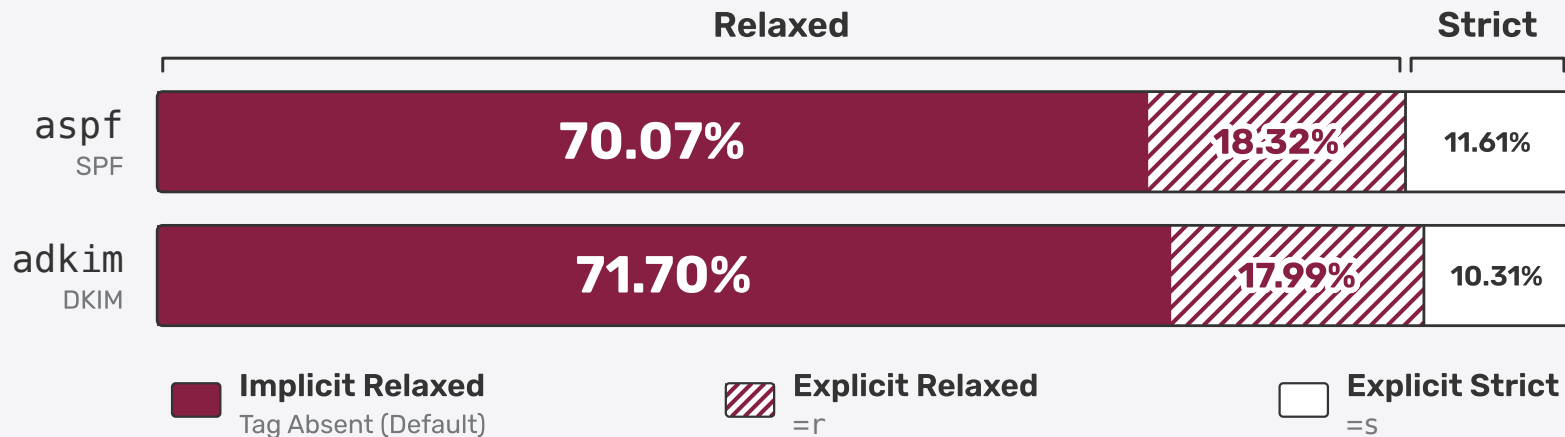
Dataset 1

DMARC In The Wild 2

Vulnerable Subdomains 3

DMARC Spoofing 4

Organizational Domains (3.2 M)



Spoofing In The Wild

Dataset 1

DMARC In The Wild 2

Vulnerable Subdomains 3

DMARC Spoofing 4

SPF all / +all

```
" v=spf1 ip4:198.51.100.10 all"
```

BreakSPF [1]

```
" v=spf1 ip4:203.0.113.25 -all "
```

DKIM Compromised Keys

```
" v=DKIM1; k=rsa; p=MIGfMA0GCSq..."
```

Vulnerable Subdomains

35 K

493 K

11

Spoofing In The Wild

Dataset 1

DMARC In The Wild 2

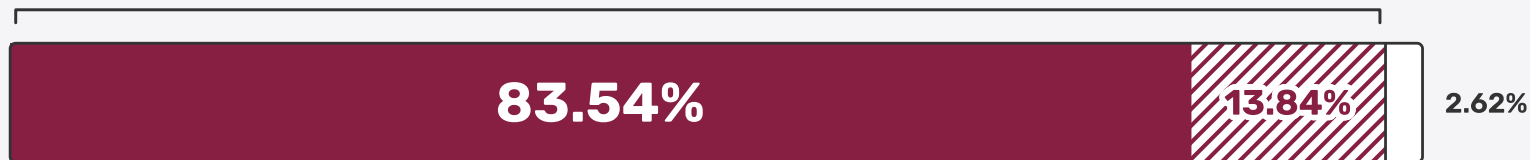
Vulnerable Subdomains 3

DMARC Spoofing 4

81 K Domain Hierarchies

With a Vulnerable Subdomain

Relaxed



Implicit Relaxed

Tag Absent (Default)



Explicit Relaxed

=r



Explicit Strict

=s

DMARC In Email Service Provider Docs

Email Service	DMARC Explained	Alignment Explained	Alignment Recommended
Google	✓	✓	Mixed
Mailgun	✓	✓	Relaxed
Amazon SES	✓	✓	Relaxed
Twilio	✓	✓	Relaxed
Mailjet	✓	✓	Relaxed
MailChannels	✓	✓	None
MailChimp	✓	✓	None
Outlook	✓	✗	None
Salesforce	✓	✗	None
SMTP2GO	✓	✗	None
Dotdigital	✓	✗	None

Learnings



Weaknesses in SPF are common despite being well-known.



DMARC inherits SPF's weaknesses by design.



Relaxed alignment propagates vulnerabilities to the entire domain hierarchy.



Email Service Providers fail to recommend secure configurations.



DKIM is more secure by design and in practice.

Can we fix the root cause without disrupting the email ecosystem?

Split Alignment

A configuration technique that provides



Security

Protects established Visible Domains from all SPF failures.

By entirely removing DMARC's dependence on SPF.



Deliverability

Preserves normal email delivery behavior for benign emails.

Verified in practice across email services.



Deployability

Deployable today with minor changes to existing protocol policies.

Already compliant with the DMARC specification and 3rd-party ESPs.

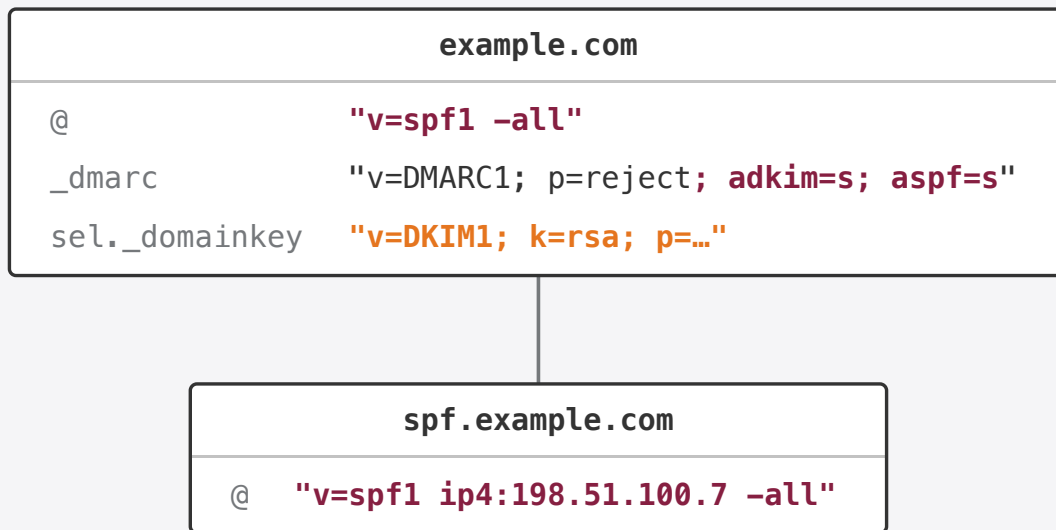
Why Not Just Strict Alignment?

	Secure Against			3rd-Party Senders
	Own SPF	Hierarchy SPF	Hierarchy DKIM	
Relaxed	✗	✗	✗	✓
Strict	✗	✓	✓	✗
Split	✓	✓	✓	✓

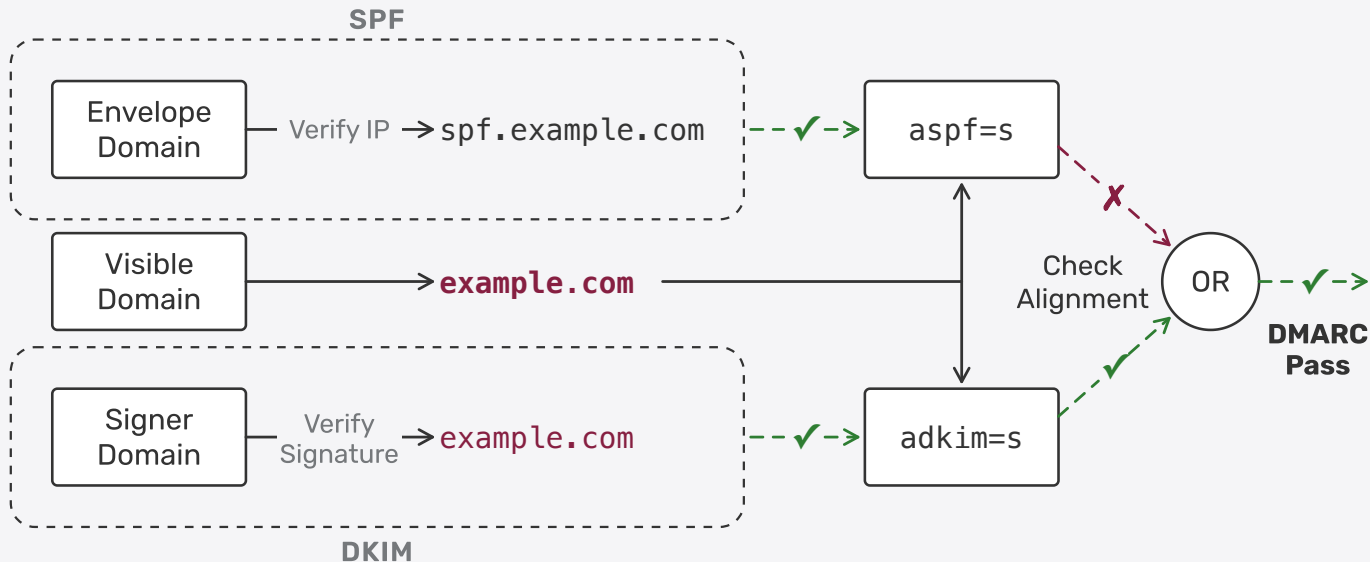
Split Alignment: secure, and compatible.

Split Alignment

- 1 Set DMARC alignment to strict.
- 2 Relocate SPF to a dedicated subdomain.
- 3 Make the Visible Domain's SPF maximally restrictive.
- 4 Deploy DKIM on the Visible Domain and sign email bodies.

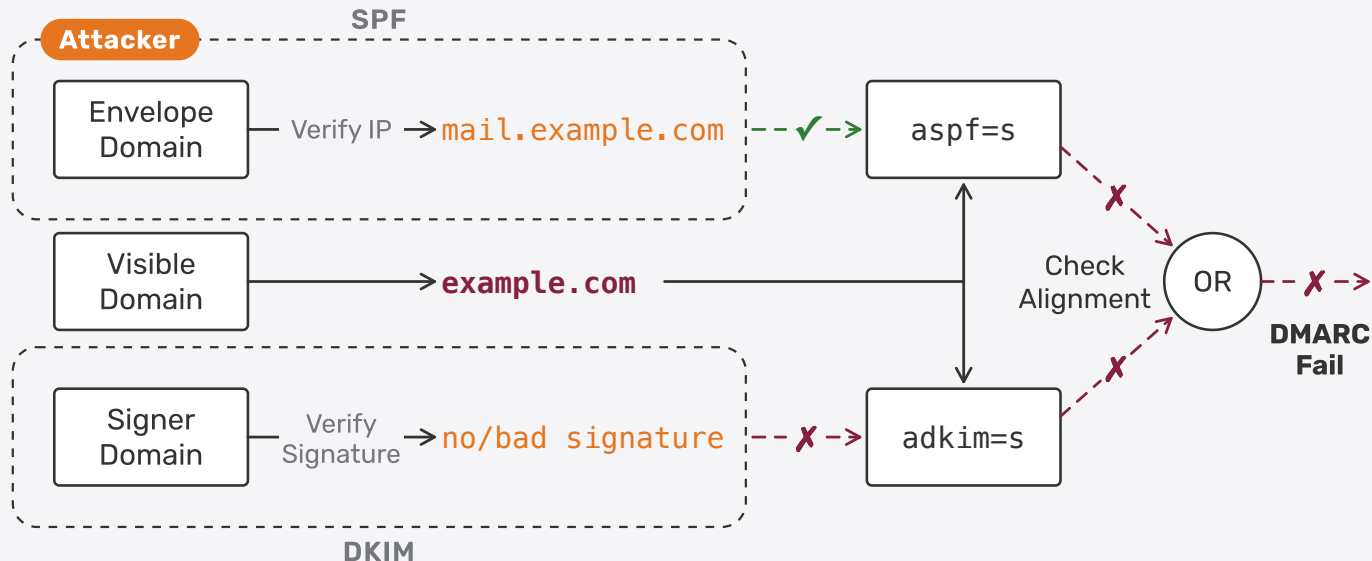


Split Alignment



- ✓ Email is still SPF authenticated, for receivers that rely on it.
- ✗ SPF fails alignment, so DMARC never uses it.
- ✓ Email is DKIM authenticated.
- ✓ The DKIM domain aligns, and DMARC relies on it.

Split Alignment



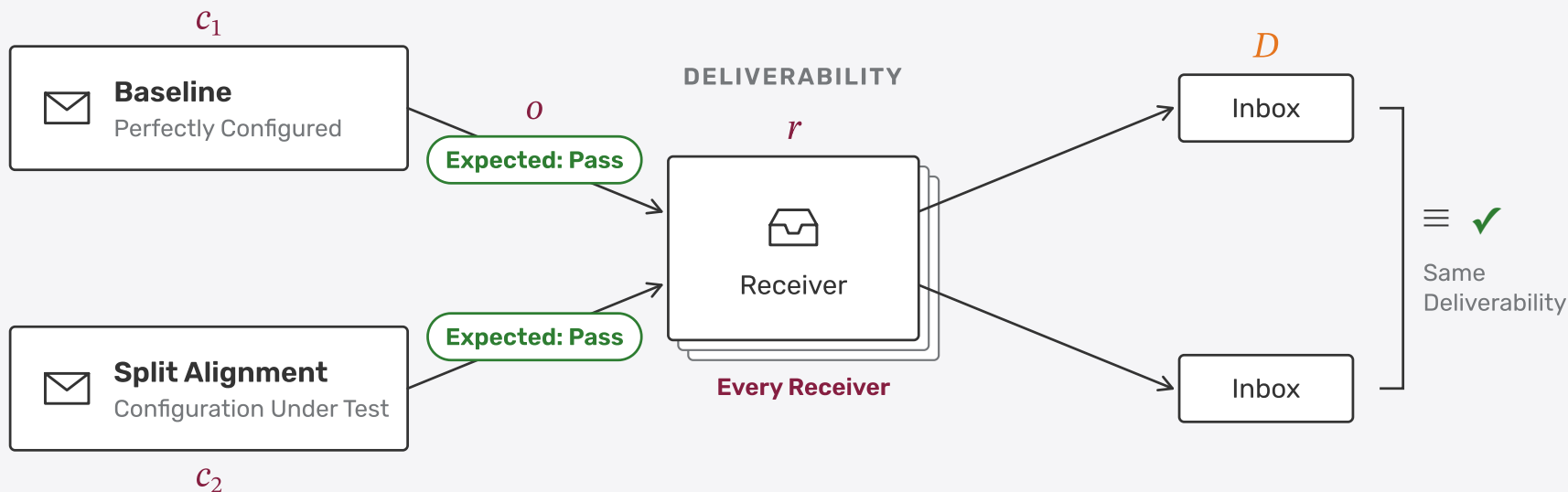
X An attacker with a subdomain's SPF cannot align, and DMARC fails.

Evaluating Split Alignment

			
 DMARC-Passing	Inbox	Spam	Inbox
 DMARC-Failing	Rejected	Rejected	Spam

Evaluating Split Alignment

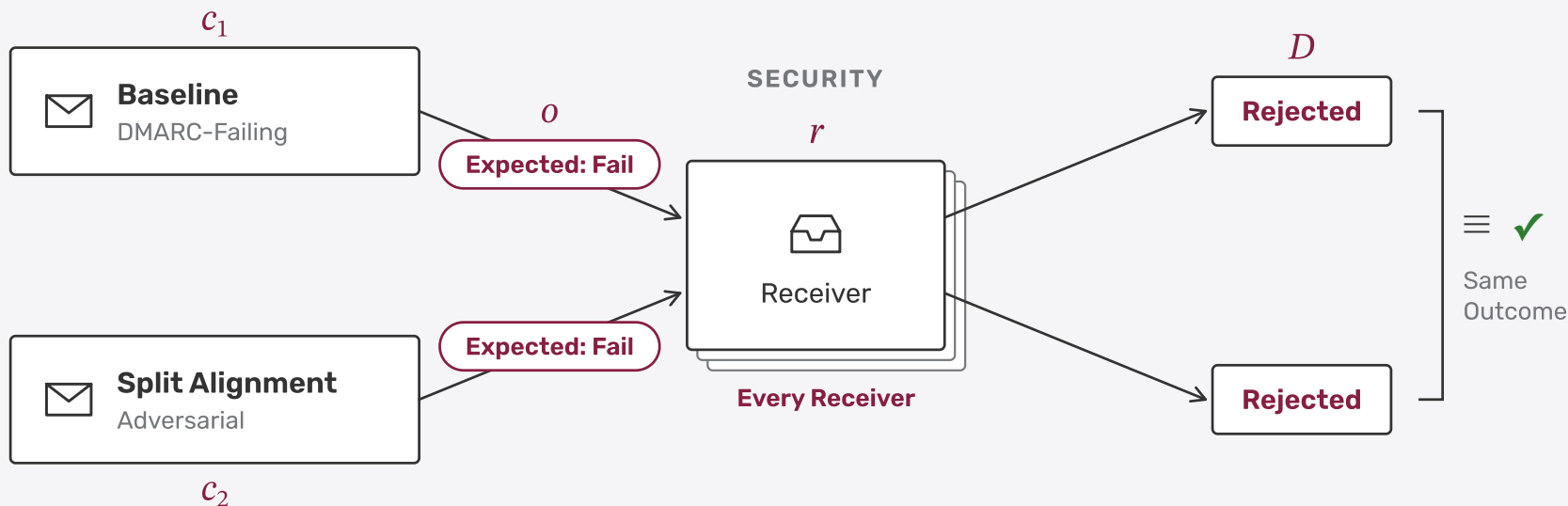
We evaluate deliverability through differential comparison within each receiver.



$$D(c_1, r, o) \equiv D(c_2, r, o)$$

Evaluating Split Alignment

We evaluate security through differential comparison within each receiver.



$$D(c_1, r, o) \equiv D(c_2, r, o)$$

Evaluating Split Alignment

Visible Domain	Deliverability		Security	
	Org.	Sub.	Org.	Sub.
gmail.com	✓ _i	✓ _i	✓ _r	✓ _r
outlook.com	✓ _s	✓ _s	✓ _r	✓ _r
proton.me	✓ _i	✓ _i	▲ _i → ✓ _s	✓ _s
yahoo.com	✓ _i	✓ _i	✓ _r	✓ _r
aol.com	✓ _i	✓ _i	✓ _r	✓ _r
zoho.com	✓ _i	✓ _i	✓ _r	✓ _r
naver.com	✓ _i	✓ _i	▲ _i → ✓ _b	✓ _b
tuta.com	✓ _i	✓ _i	✓ _s	▲ _i → ✓ _s
onet.pl	✓ _i	✓ _i	✓ _r	✓ _r
yandex.com	✓ _s	✓ _s	✓ _w	✓ _w
mailo.com	✓ _i	✓ _i	✓ _r	✓ _r
mail.com	✓ _i	✓ _i	✓ _s	✓ _s
inbox.lv	✓ _i	✓ _i	✓ _s	✓ _s
sapo.pt	✓ _i	✓ _i	✓ _r	✓ _r
seznam.cz	✓ _i	✓ _i	▲ _s → *	✓ _b

Takeaways



ESPs & Senders

ESPs should recommend Split Alignment, and senders should adopt it to secure themselves.



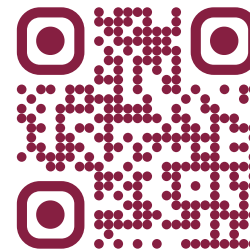
Email Receivers

Implement protocols to specification and treat SPF passes with caution.

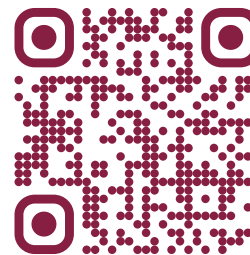


Researchers

Use the generalized measurement and evaluation techniques introduced in this paper to improve the security of the email ecosystem.



WEBSITE



PAPER