Split Alignment

Diffusing SPF Vulnerabilities with DMARC

Muhammad Hamza[1], Mattijs Jonker[2], Raffaele Sommese[2], Simon Fernandez[3], Olivier Hureau[3], Eric Pauley[1,4], Taejoong Chung[1]

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

Email Spoofing



Email Spoofing

IMC 2023 • Czybik et al.

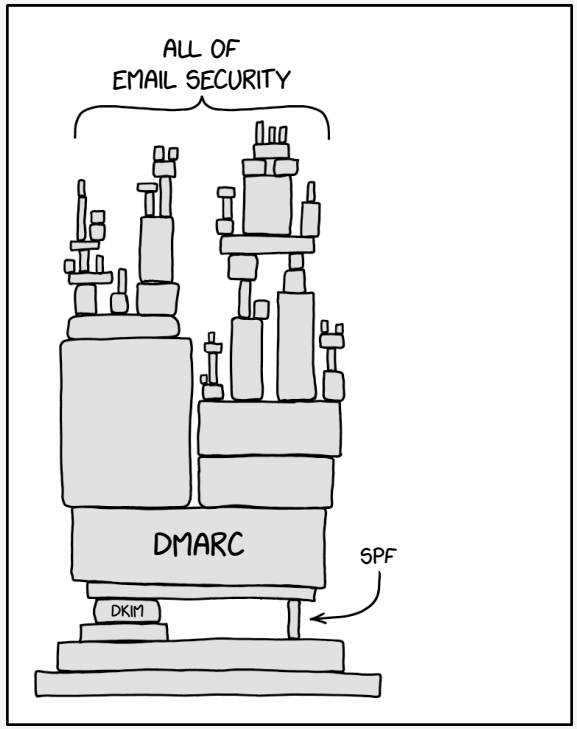
Lazy Gatekeepers: A Large-Scale Study on SPF Configuration in the Wild

USENIX SECURITY 2024 • Ashiq et al.

SPF Beyond the Standard: Management and Operational Challenges in Practice and Practical Recommendations

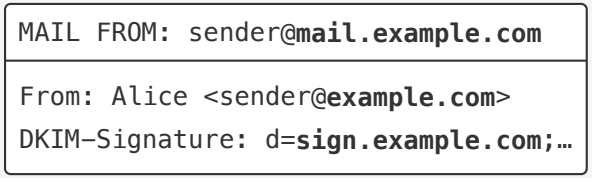
NDSS 2024 • Wang et al.

BreakSPF: How Shared Infrastructures Magnify SPF Vulnerabilities Across the Internet



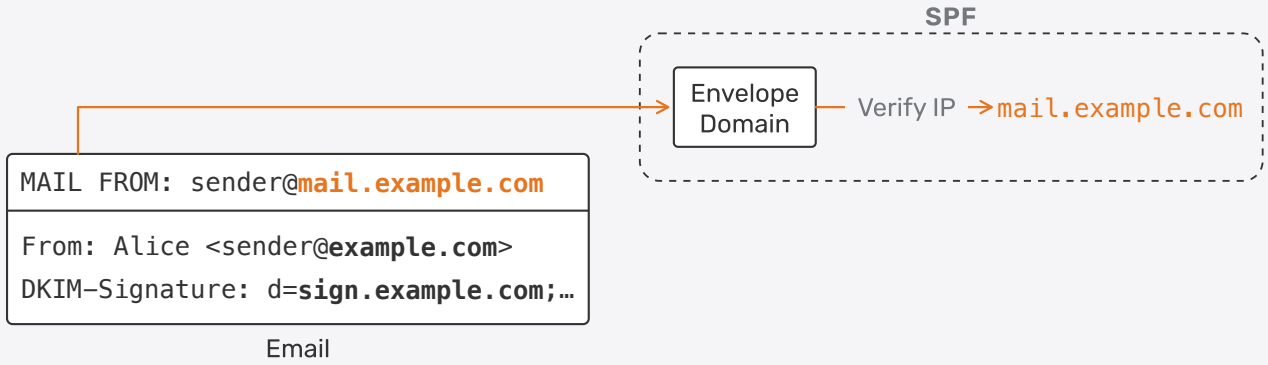
xkcd.com/2347 • Randall Munroe (CC BY-NC 2.5), adapted

Email Authentication

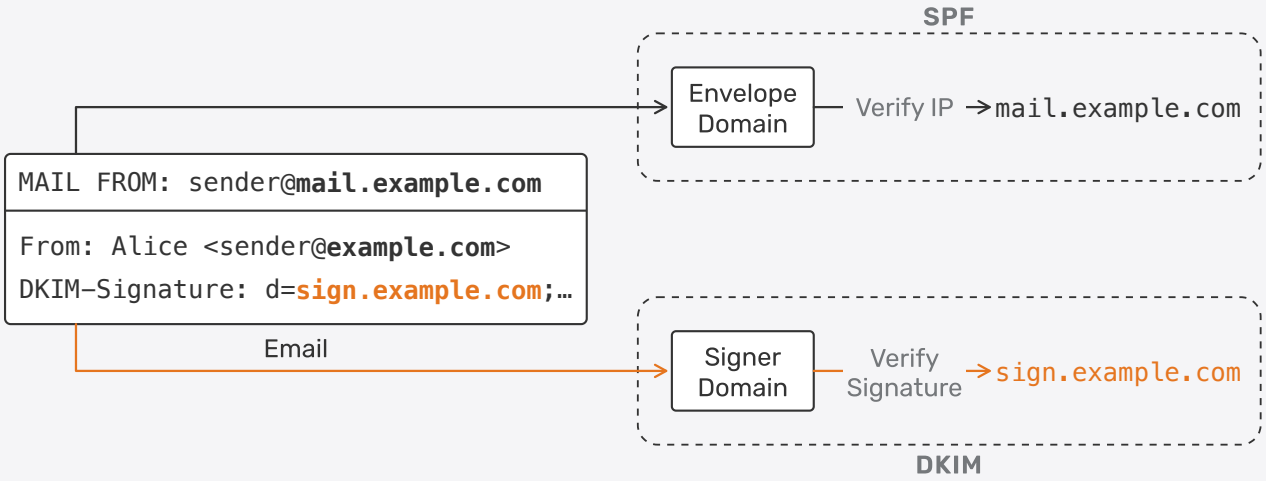


Email

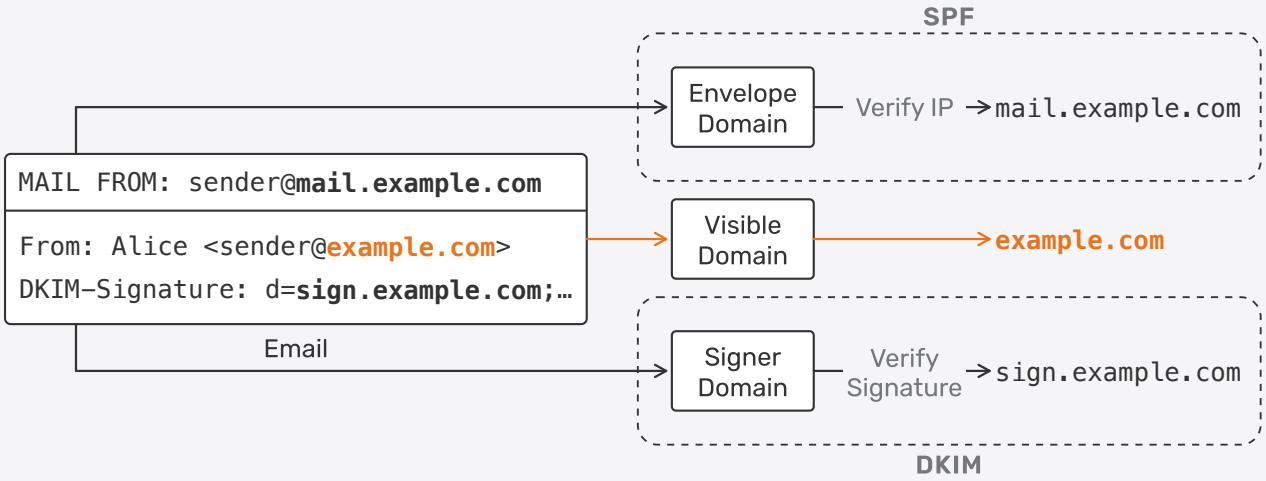
Email Authentication



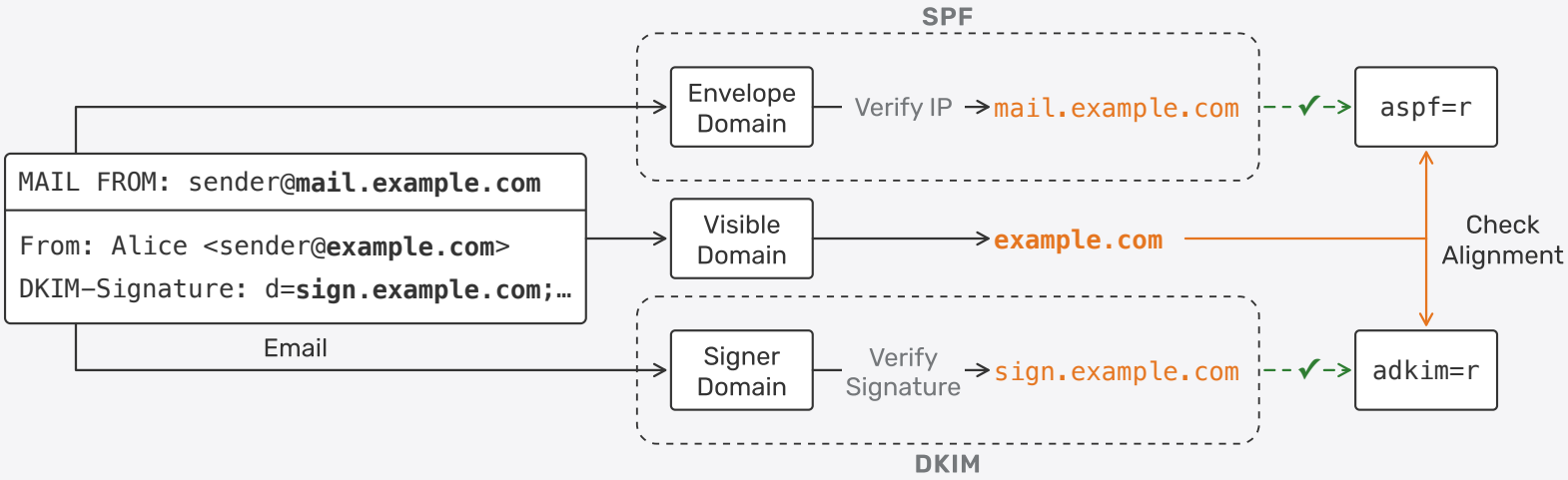
Email Authentication



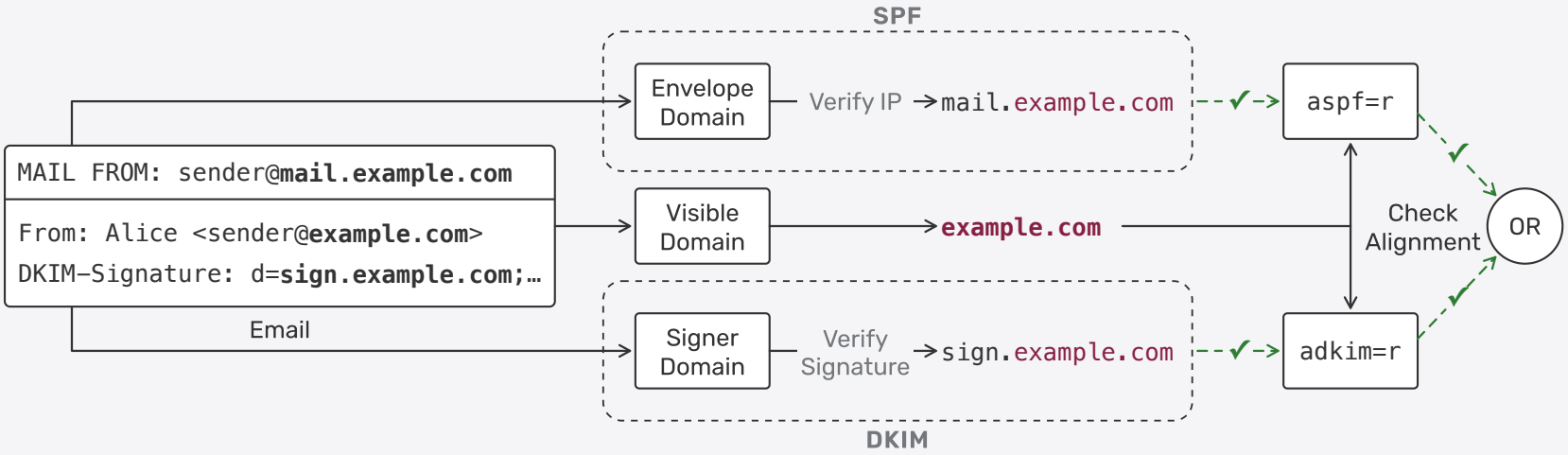
Email Authentication



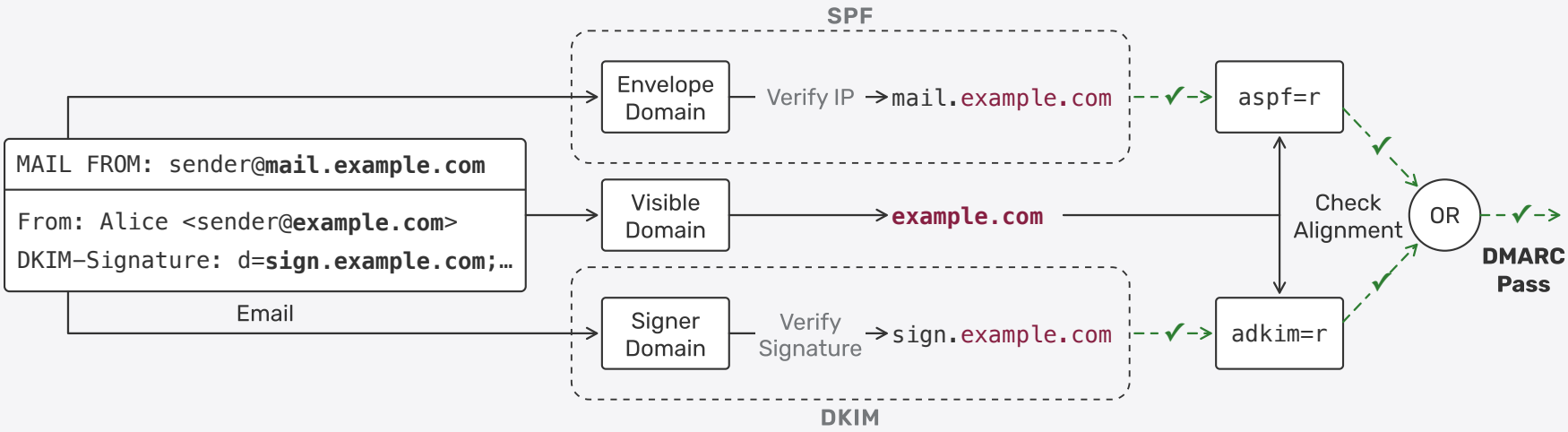
Email Authentication



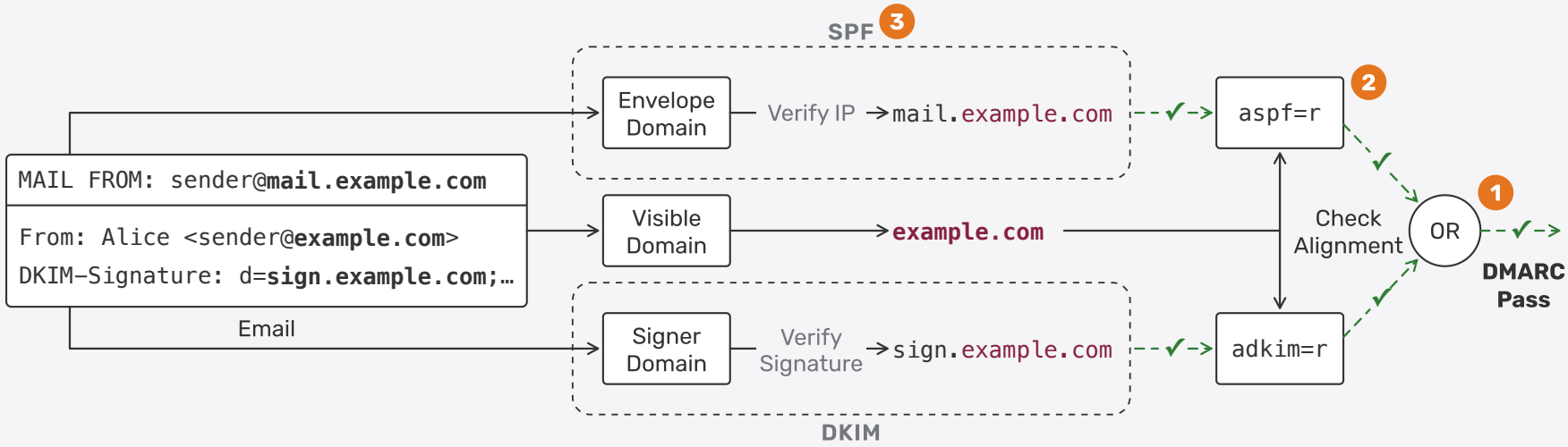
Email Authentication



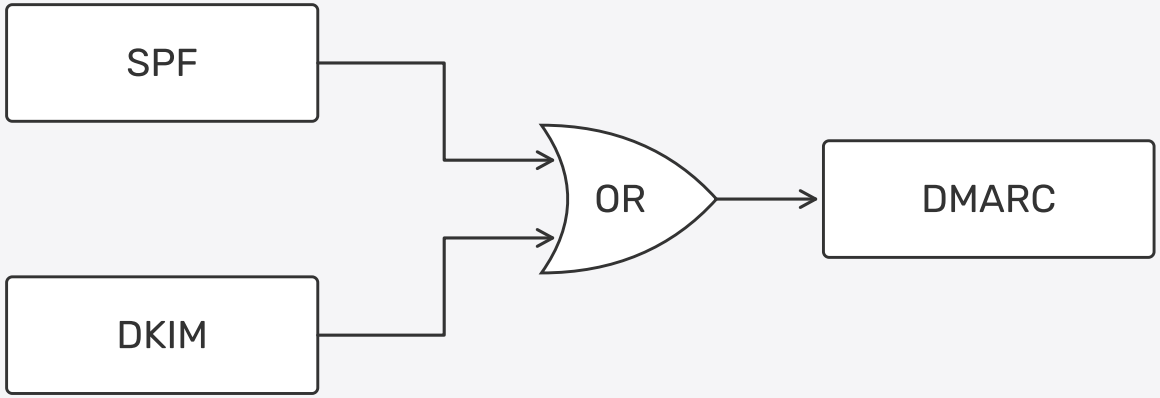
Email Authentication



Email Authentication

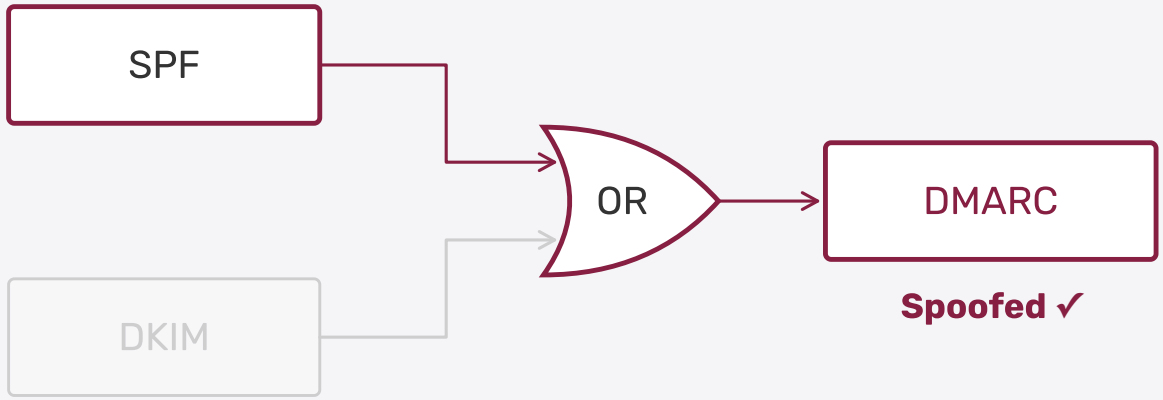


Spoofing Email Using The Weakest Link



Spoofing Email Using The Weakest Link

The weaker of the two can be used to pass DMARC



Spoofing Email Using The Weakest Link

Alignment Mode	Authenticated Domain		Visible Domain
Relaxed =r	mail.example.com	==	example.com

Spoofing Email Using The Weakest Link

Alignment Mode	Authenticated Domain		Visible Domain	
Relaxed =r	mail.example.com	==	example.com	✓**Aligned** only org. domain must match

Spoofing Email Using The Weakest Link

Alignment Mode	Authenticated Domain		Visible Domain	
Relaxed =r	mail.example.com	==	example.com	✓ **Aligned** only org. domain must match
Strict =s	mail.example.com	==	example.com	✗ **Not Aligned** whole FQDN must match

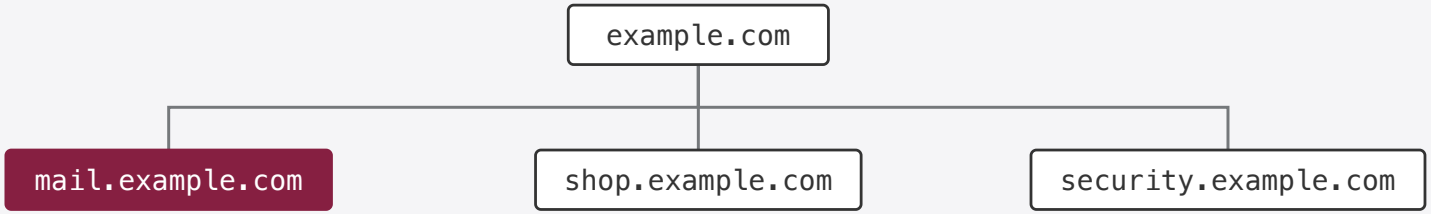
Spoofing Email Using The Weakest Link

Alignment Mode	Authenticated Domain		Visible Domain	
Relaxed `=r` **(default)**	`mail.example.com`	==	`example.com`	**✓ Aligned** only org. domain must match
Strict `=s`	`mail.example.com`	==	`example.com`	**✗ Not Aligned** whole FQDN must match

Spoofing Email Using The Weakest Link

Alignment Mode	Authenticated Domain		Visible Domain	
Relaxed `=r` **(default)**	`mail.example.com`	==	`example.com`	✓**Aligned** only org. domain must match

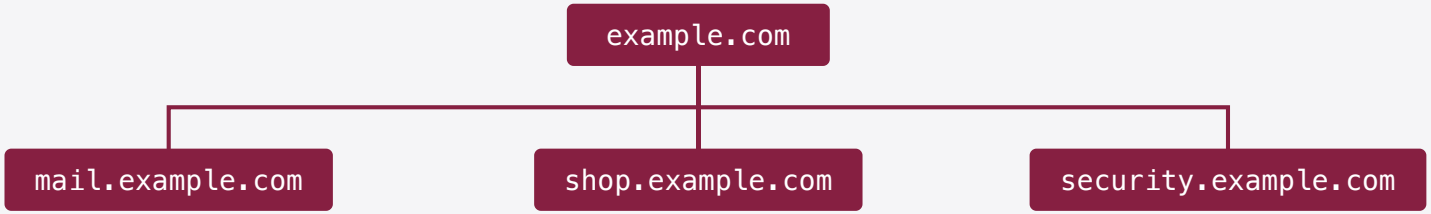
By default, `mail.example.com` can authenticate for any domain in the hierarchy



Spoofing Email Using The Weakest Link

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


```
bad-spf.example.com. TXT
"v=spf1  ip4:203.0.113.25  ip6:2001:db8::/32  include:spf.thirdparty.com  all"
```

Spoofing Email Using The Weakest Link


```
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.

Spoofing Email Using The Weakest Link


```
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.

Spoofing Email Using The Weakest Link


```
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

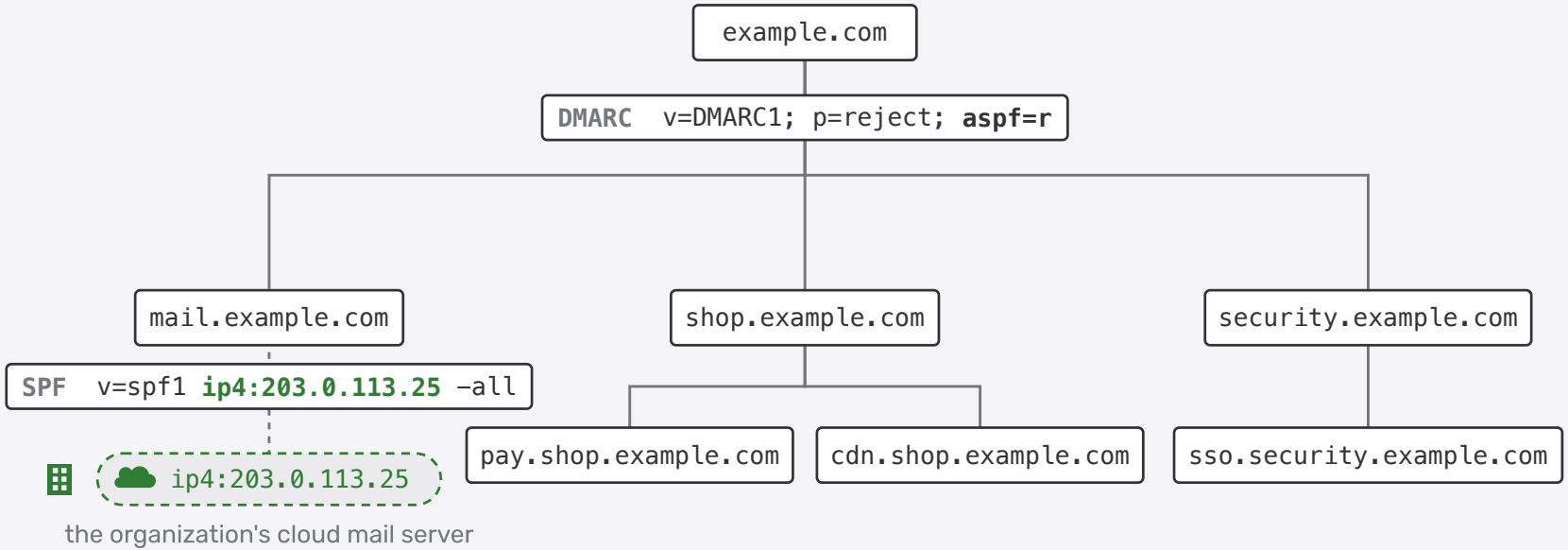
Broad CIDR ranges and chains of includes authorize far more senders than intended.

Permissive By Default

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

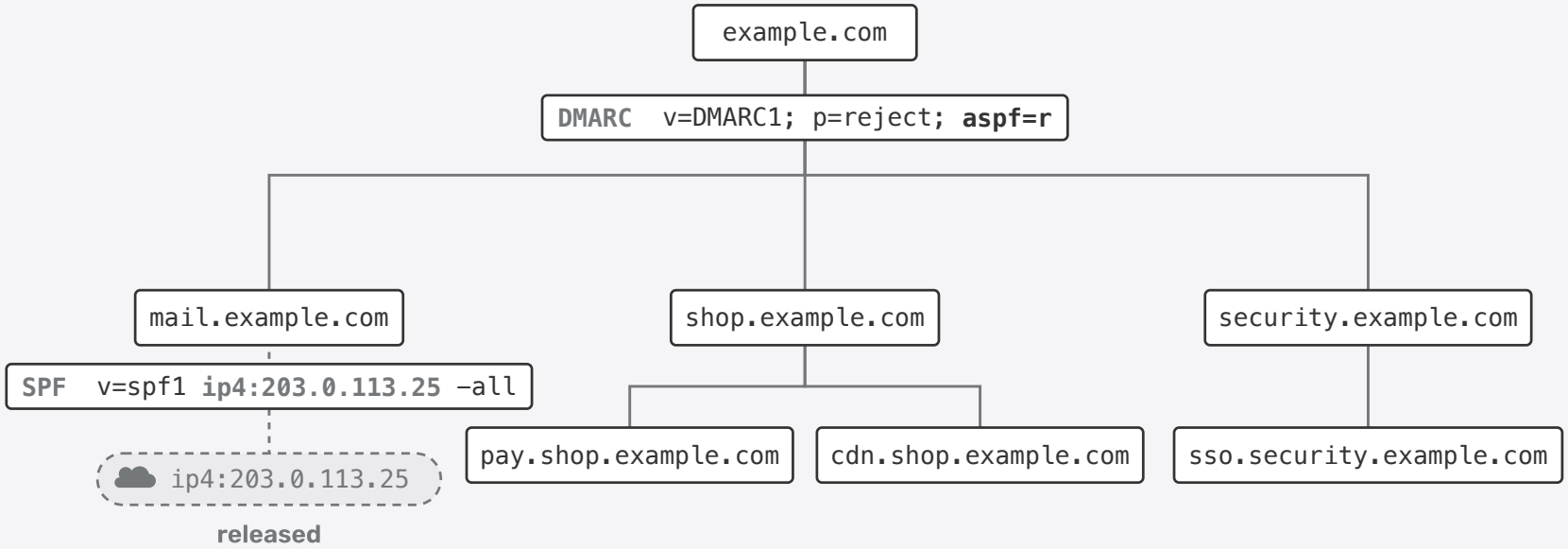
Spoofing Email Using The Weakest Link

OR Clause 1
Relaxed Alignment 2
SPF 3



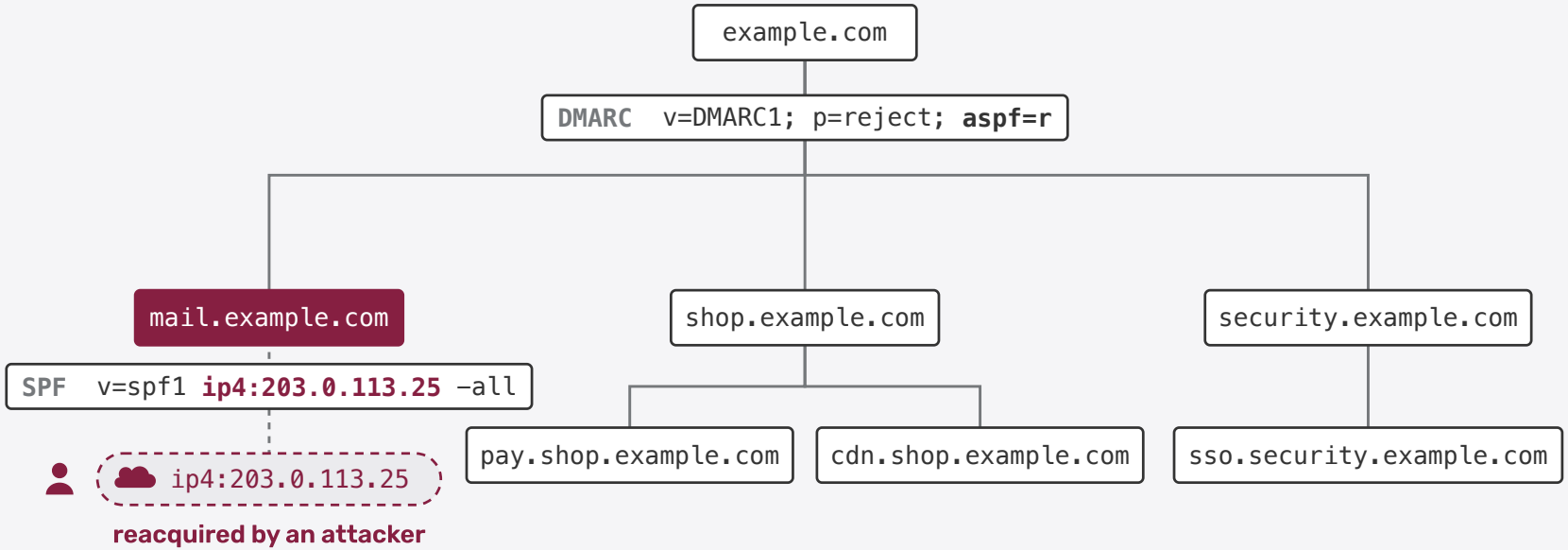
Spoofing Email Using The Weakest Link

OR Clause 1
Relaxed Alignment 2
SPF 3



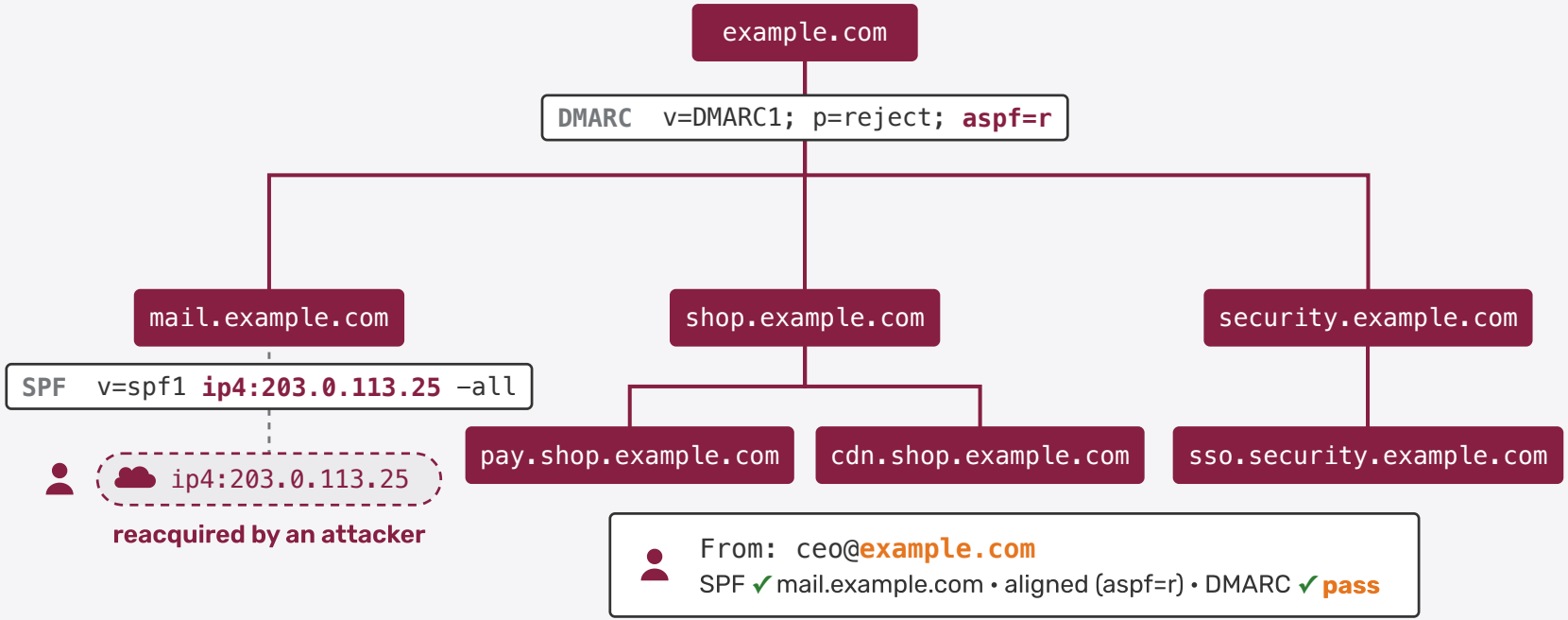
Spoofing Email Using The Weakest Link

OR Clause 1
Relaxed Alignment 2
SPF 3



Spoofing Email Using The Weakest Link

OR Clause 1
Relaxed Alignment 2
SPF 3



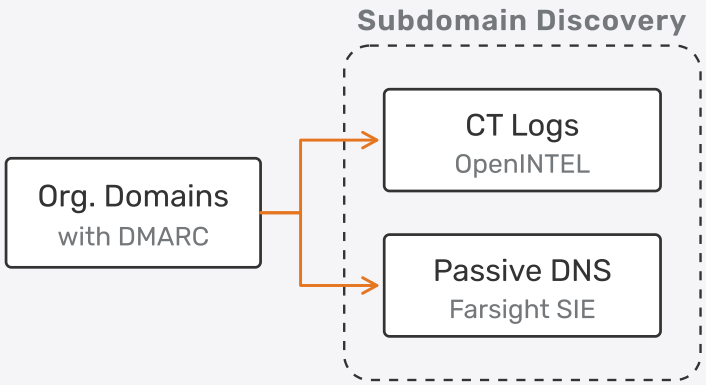
Spoofing In The Wild

Dataset 1
DMARC In The Wild 2
Vulnerable Subdomains 3
DMARC Spoofing 4

Org. Domains
with DMARC

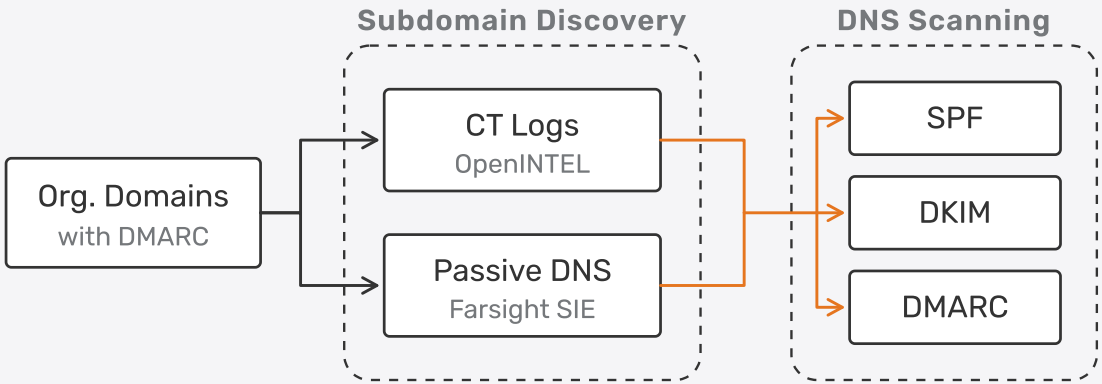
Spoofing In The Wild

Dataset 1
DMARC In The Wild 2
Vulnerable Subdomains 3
DMARC Spoofing 4



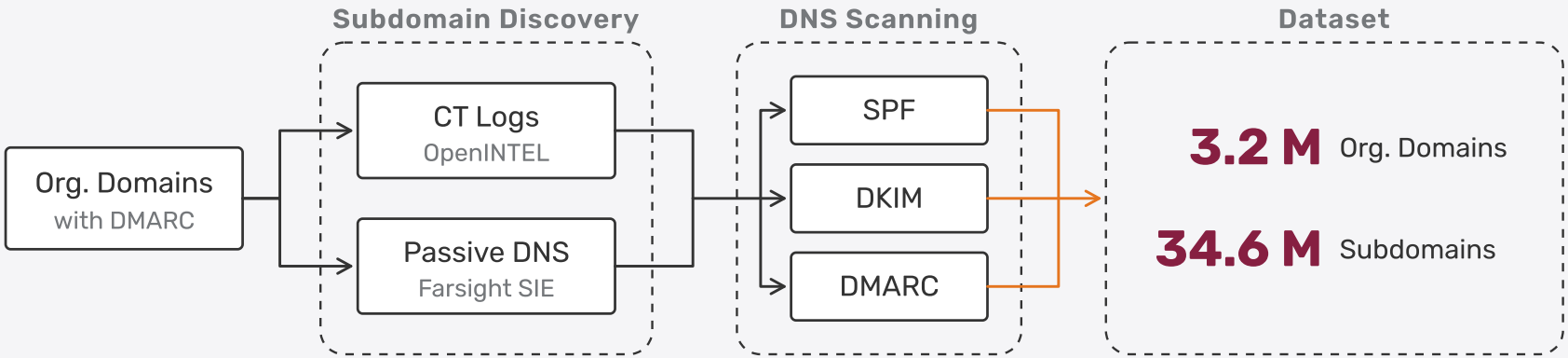
Spoofing In The Wild

Dataset 1
DMARC In The Wild 2
Vulnerable Subdomains 3
DMARC Spoofing 4



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

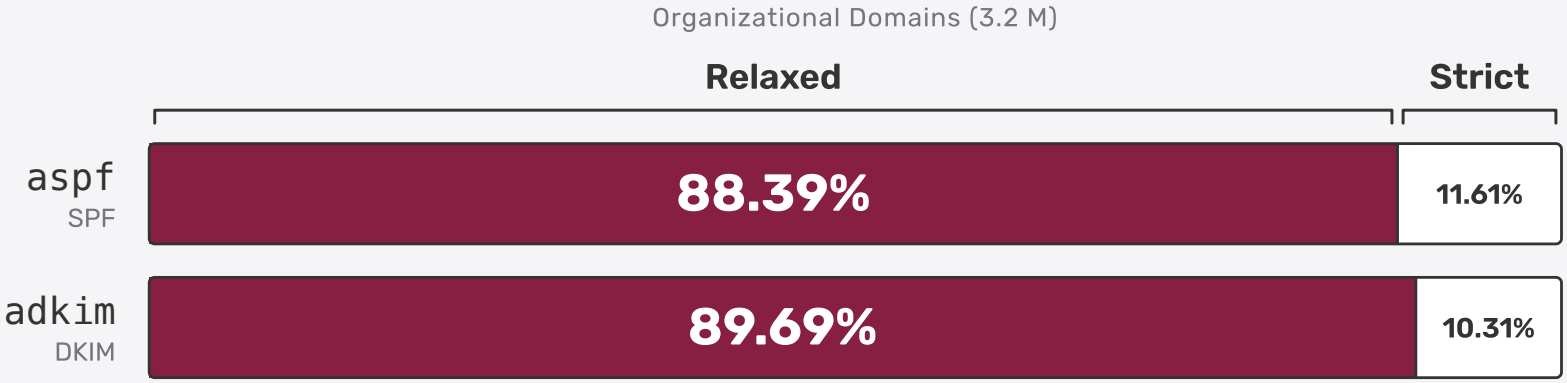
Organizational Domains (3.2 M)

`aspf`
SPF

`adkim`
DKIM

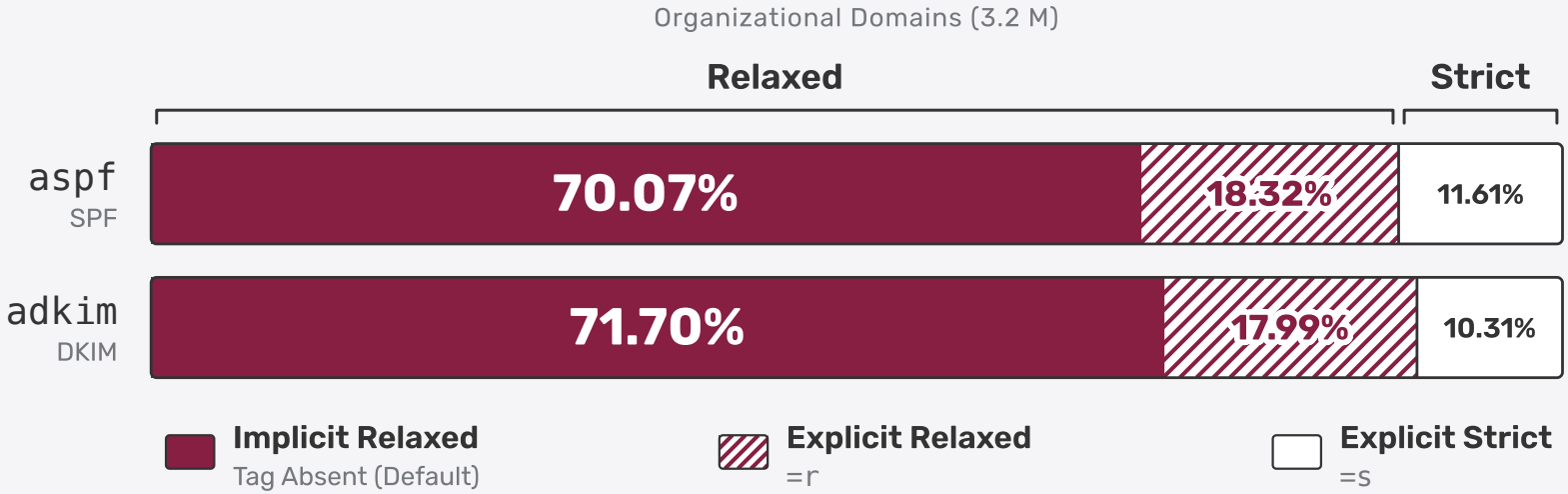
Spoofing In The Wild

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



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

[1] C. Wang et al., "BreakSPF: How Shared Infrastructures Magnify SPF Vulnerabilities Across the Internet," NDSS, 2024. doi.org/10.14722/ndss.2024.23113

Spoofing In The Wild

SPF all / +all

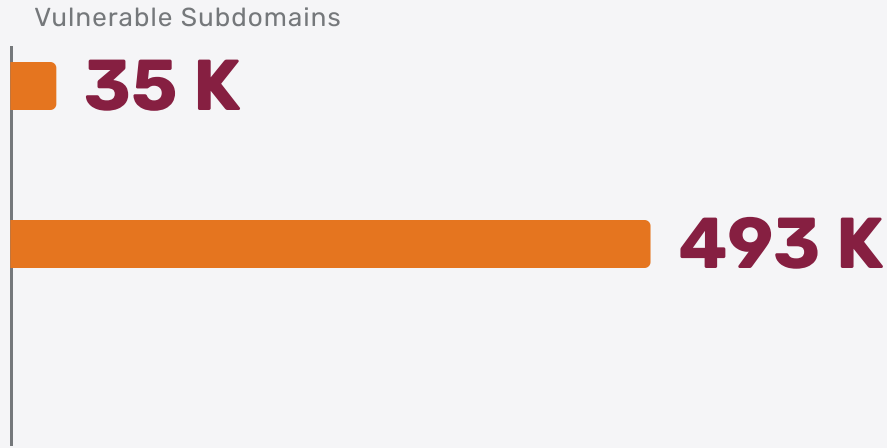
```
" v=spf1  ip4:198.51.100.10 all"
```

BreakSPF [1]

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

DKIM Compromised Keys

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



[1] C. Wang et al., "BreakSPF: How Shared Infrastructures Magnify SPF Vulnerabilities Across the Internet," NDSS, 2024. doi.org/10.14722/ndss.2024.23113

Spoofing In The Wild

Dataset 1
DMARC In The Wild 2
Vulnerable Subdomains 3
DMARC Spoofing 4

SPF all / +all

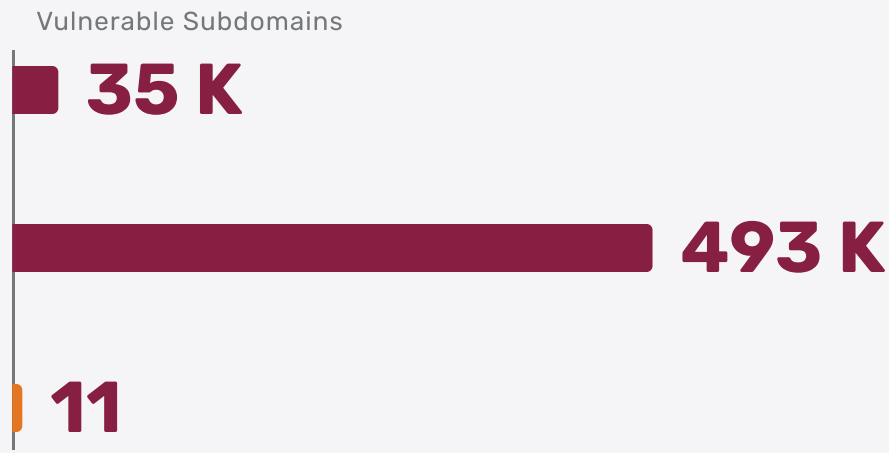
```
" v=spf1  ip4:198.51.100.10 all"
```

BreakSPF [1]

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

DKIM Compromised Keys

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



[1] C. Wang et al., "BreakSPF: How Shared Infrastructures Magnify SPF Vulnerabilities Across the Internet," NDSS, 2024. doi.org/10.14722/ndss.2024.23113

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



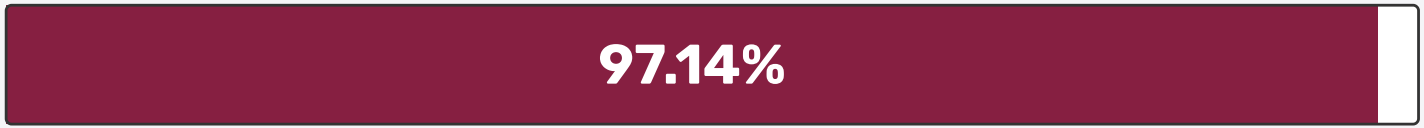
Spoofing In The Wild

Dataset 1
DMARC In The Wild 2
Vulnerable Subdomains 3
DMARC Spoofing 4

81 K Domain Hierarchies

With a Vulnerable Subdomain

79 K Entirely Spoofable

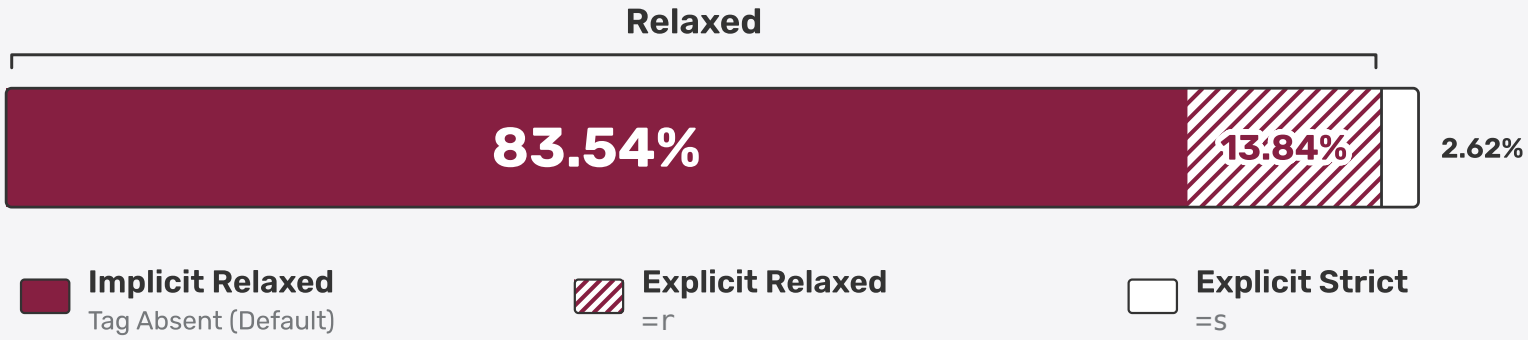


Spoofing In The Wild

Dataset 1
DMARC In The Wild 2
Vulnerable Subdomains 3
DMARC Spoofing 4

81 K Domain Hierarchies

With a Vulnerable Subdomain



DMARC In Email Service Provider Docs

Email Service
Google
Mailgun
Amazon SES
Twilio
Mailjet
MailChannels
MailChimp
Outlook
Salesforce
SMTP2GO
Dotdigital

DMARC In Email Service Provider Docs

Email Service	DMARC Explained
Google	✓
Mailgun	✓
Amazon SES	✓
Twilio	✓
Mailjet	✓
MailChannels	✓
MailChimp	✓
Outlook	✓
Salesforce	✓
SMTP2GO	✓
Dotdigital	✓

DMARC In Email Service Provider Docs

Email Service	DMARC Explained	Alignment Explained
Google	✓	✓
Mailgun	✓	✓
Amazon SES	✓	✓
Twilio	✓	✓
Mailjet	✓	✓
MailChannels	✓	✓
MailChimp	✓	✓
Outlook	✓	✗
Salesforce	✓	✗
SMTP2GO	✓	✗
Dotdigital	✓	✗

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

Learnings



Weaknesses in SPF are common despite being well-known.

Learnings

Weaknesses in SPF are common despite being well-known.

DMARC inherits SPF's weaknesses by design.

Learnings

- Weaknesses in SPF are common despite being well-known.
- DMARC inherits SPF's weaknesses by design.
- DMARC's defaults propagates vulnerabilities to the entire domain hierarchy.

Learnings

- Weaknesses in SPF are common despite being well-known.
- DMARC inherits SPF's weaknesses by design.
- DMARC's defaults propagates vulnerabilities to the entire domain hierarchy.
- Email Service Providers prefer relaxed configs for deliverability.

Learnings

- Weaknesses in SPF are common despite being well-known.
- DMARC inherits SPF's weaknesses by design.
- DMARC's defaults propagates vulnerabilities to the entire domain hierarchy.
- Email Service Providers prefer relaxed configs for deliverability.
- DKIM is more secure by design and in practice.

Learnings

- Weaknesses in SPF are common despite being well-known.
- DMARC inherits SPF's weaknesses by design.
- DMARC's defaults propagates vulnerabilities to the entire domain hierarchy.
- Email Service Providers prefer relaxed configs for deliverability.
- 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

Split Alignment

A configuration technique that provides

Security	Protects established Visible Domains from all SPF failures.	**By entirely removing DMARC's dependence on SPF.**

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.**

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			
	Own SPF	Hierarchy SPF	Hierarchy DKIM	3rd-Party Senders
Relaxed r	✗	✗	✗	✓

Why Not Just Strict Alignment?

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

Strict breaks third-party senders: they put the bounce address on a subdomain.

Why Not Just Strict Alignment?

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

And strict still trusts the Visible Domain's own SPF.

Why Not Just Strict Alignment?

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

Split Alignment: secure, and compatible.

Why Not Neutral Or No SPF?

No SPF
`none`

Neutral SPF
`?all`

Why Not Neutral Or No SPF?

	Bulk Sender Rules
No SPF `none`	✗
Neutral SPF `?all`	✗

Large ESPs require email from bulk senders to be both SPF and DKIM authenticated. [1, 2]

[1] Google, “Email sender guidelines,” Gmail Help. support.google.com/a/answer/81126
[2] Yahoo, “Sender Best Practices,” Yahoo Sender Hub. senders.yahooinc.com/best-practices

Why Not Neutral Or No SPF?

	Bulk Sender Rules	Spam Filtering
No SPF `none`	✗	✗
Neutral SPF `?all`	✗	✗

Receivers may use SPF results for spam detection.

Why Not Neutral Or No SPF?

	Bulk Sender Rules	Spam Filtering	Legacy Infrastructure
No SPF `none`	✗	✗	✗
Neutral SPF `?all`	✗	✗	✗

Older infrastructure may rely on SPF.

Why Not Neutral Or No SPF?

	Bulk Sender Rules	Spam Filtering	Legacy Infrastructure
No SPF `none`	✗	✗	✗
Neutral SPF `?all`	✗	✗	✗
Split `pass`	✓	✓	✓

Split Alignment: supports all cases.

Split Alignment

example.com

```
@        "v=spf1 ip4:198.51.100.7 -all"
_dmarc   "v=DMARC1; p=reject"
```

Split Alignment

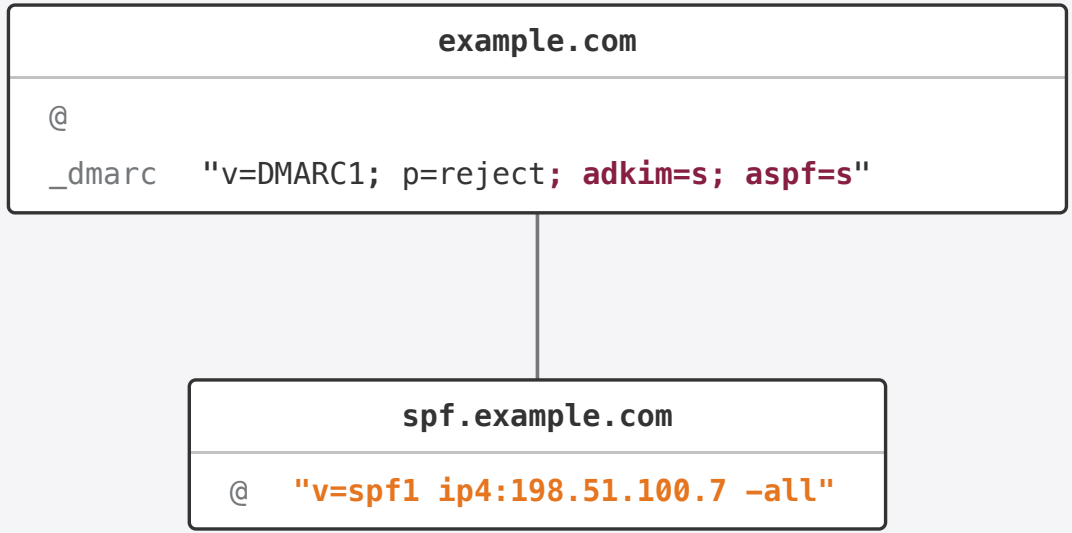
1. Set DMARC alignment to strict.

example.com

```
@        "v=spf1 ip4:198.51.100.7 -all"
_dmarc   "v=DMARC1; p=reject; adkim=s; aspf=s"
```

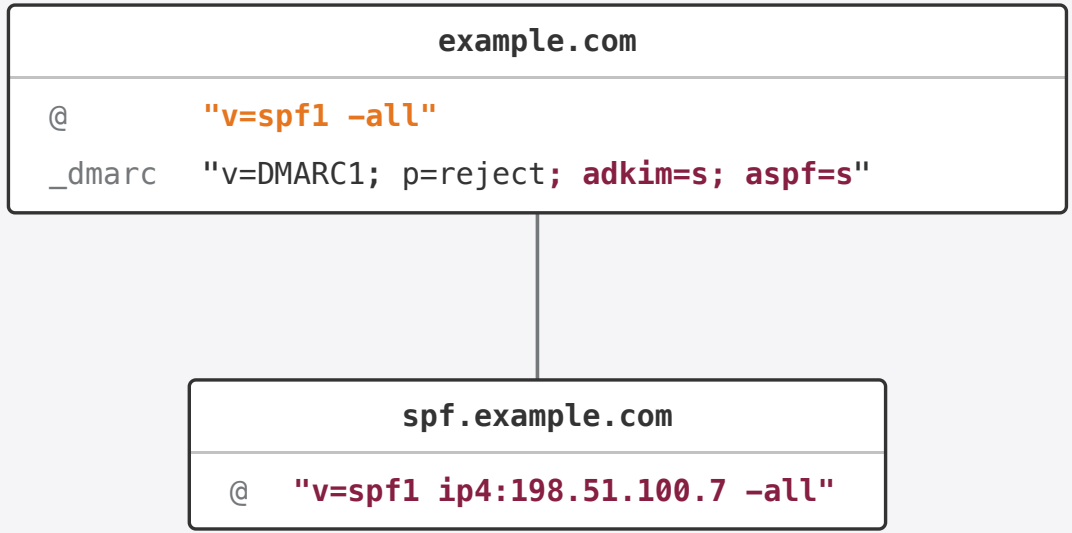
Split Alignment

1. Set DMARC alignment to strict.
2. Relocate SPF to a dedicated subdomain.



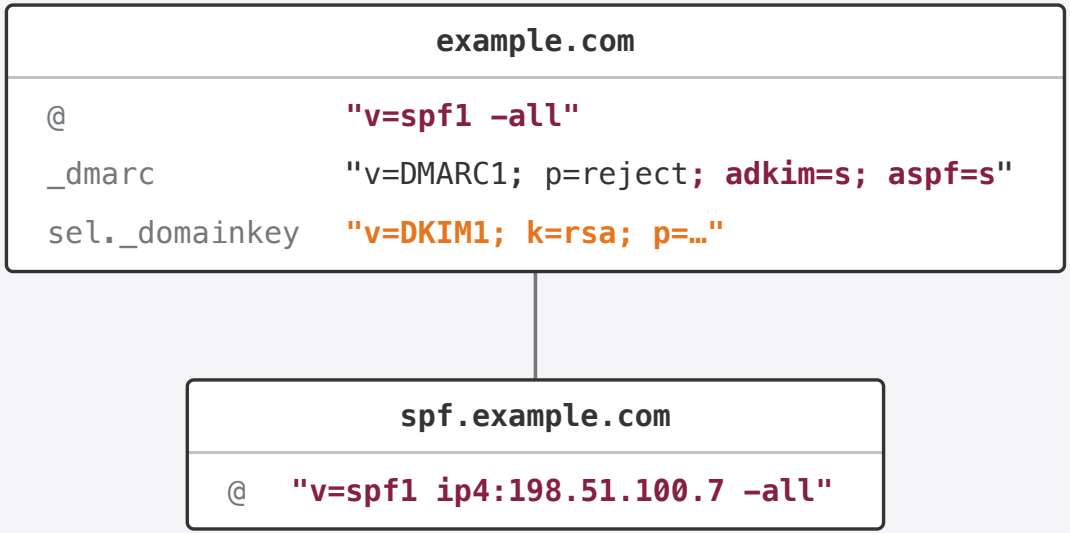
Split Alignment

1. Set DMARC alignment to strict.
2. Relocate SPF to a dedicated subdomain.
3. Make the Visible Domain's SPF maximally restrictive.

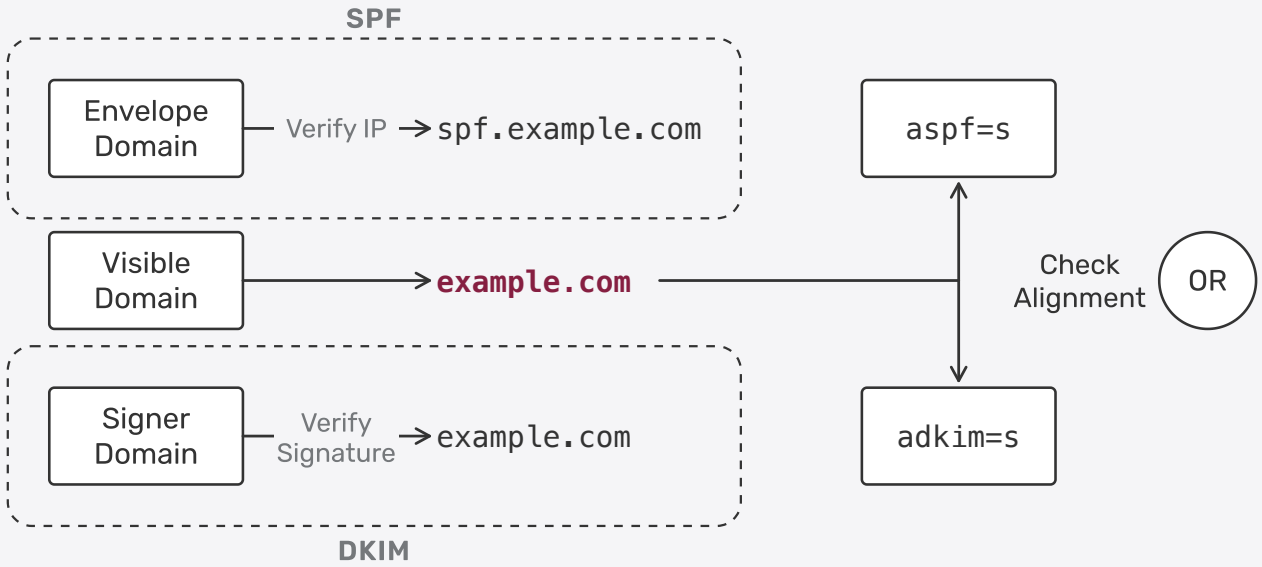


Split Alignment

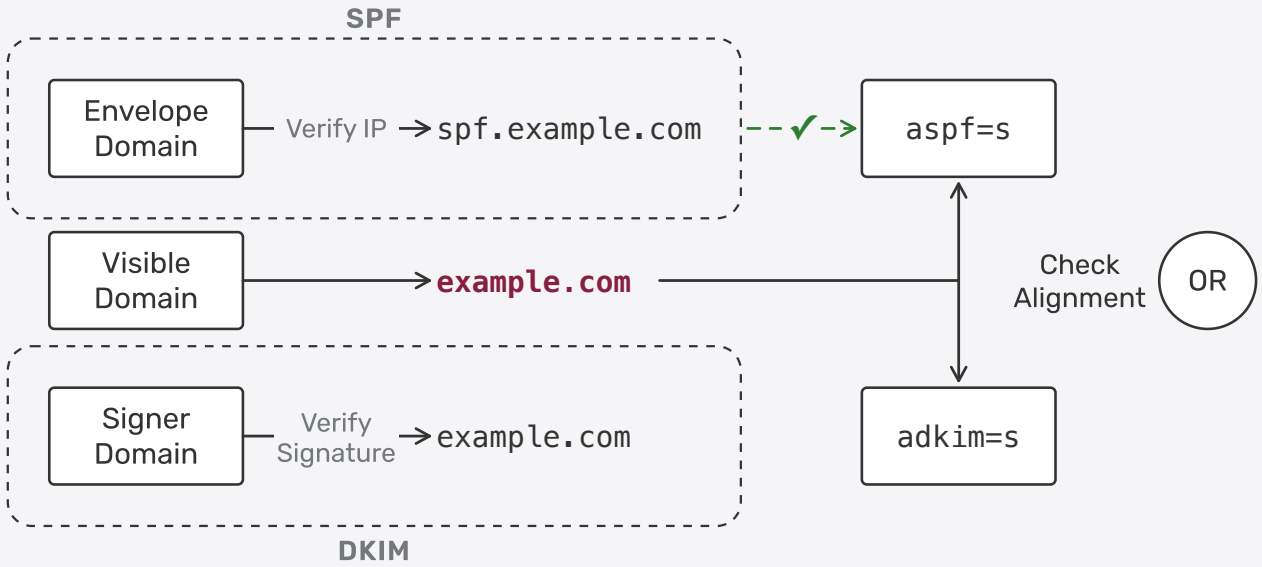
1. Set DMARC alignment to strict.
2. Relocate SPF to a dedicated subdomain.
3. Make the Visible Domain's SPF maximally restrictive.
4. Deploy DKIM on the Visible Domain and sign email bodies.



Split Alignment

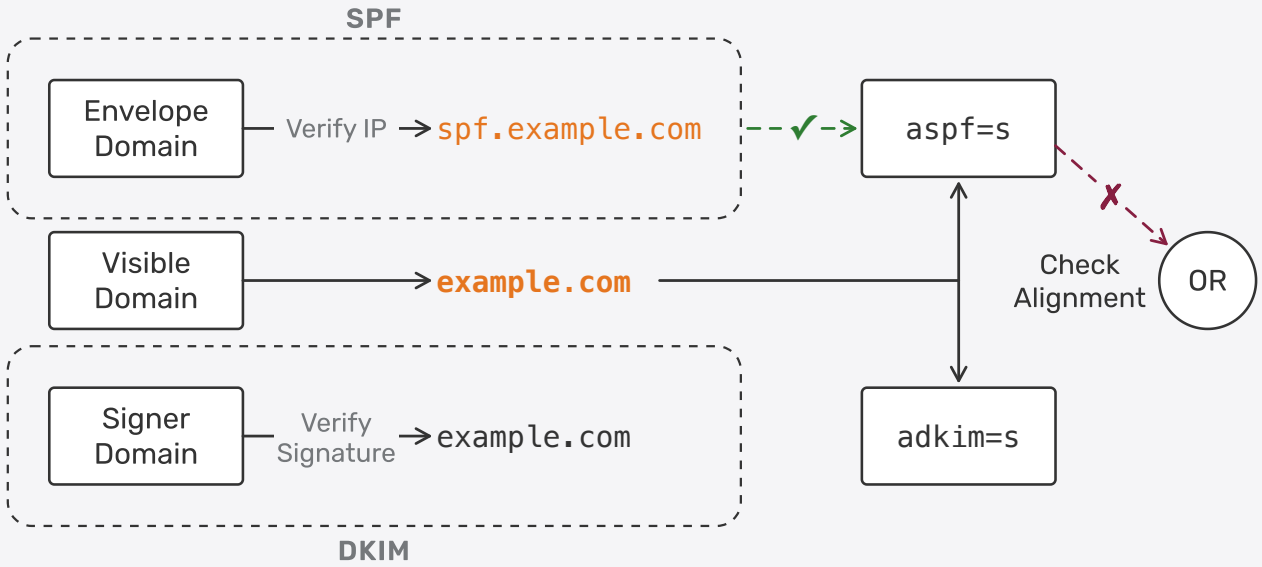


Split Alignment



✓ **Email is still SPF authenticated, for receivers that rely on it.**

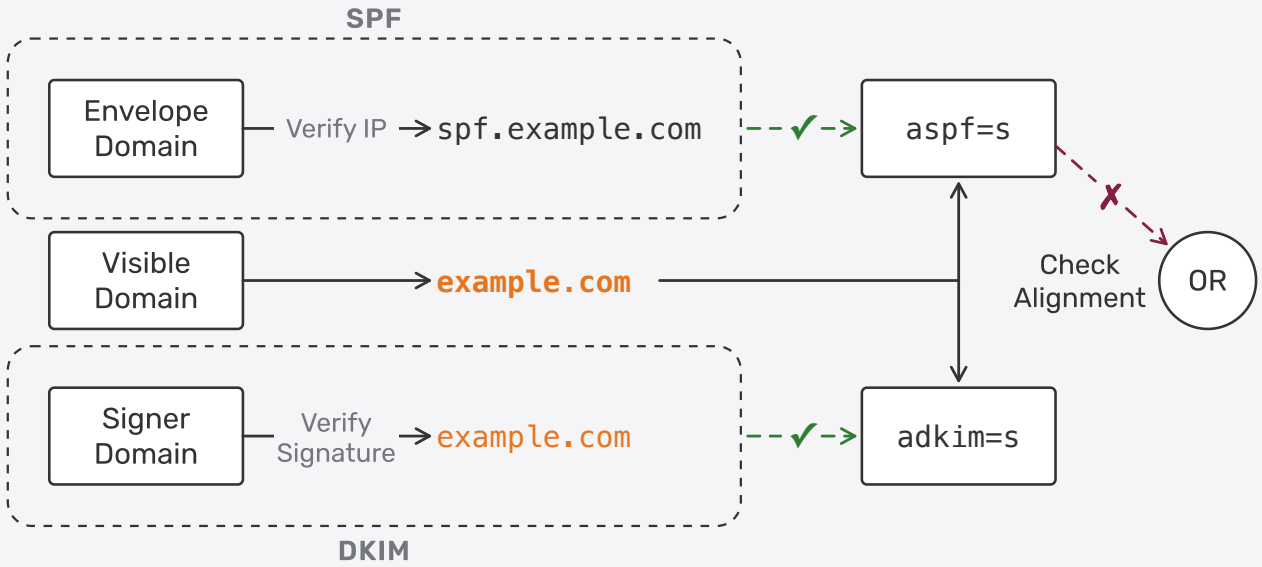
Split Alignment



✓ Email is still SPF authenticated, for receivers that rely on it.

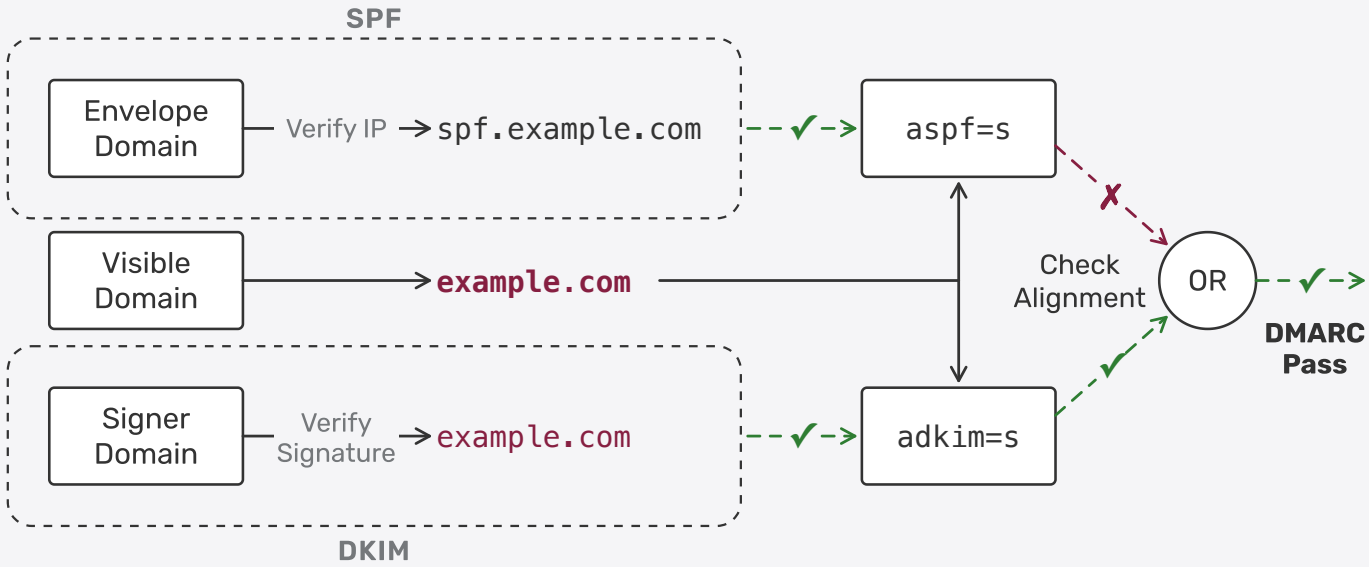
✗ SPF fails alignment, so DMARC never uses it.

Split Alignment



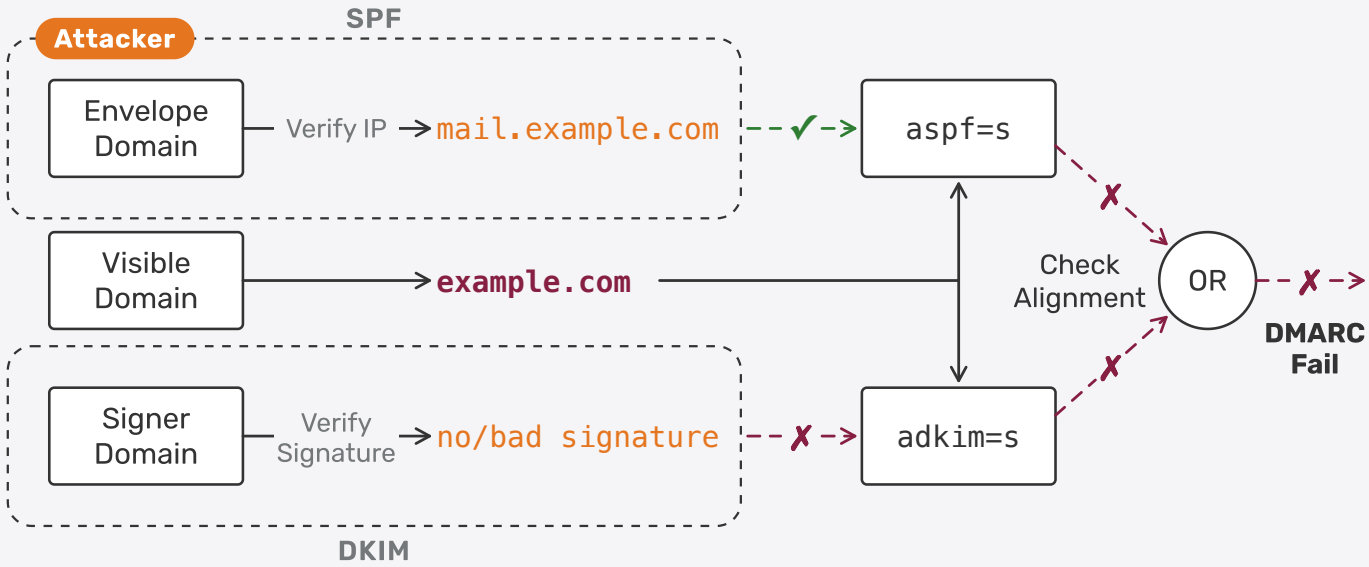
- ✓ Email is still SPF authenticated, for receivers that rely on it.
- ✗ SPF fails alignment, so DMARC never uses it.
- ✓ Email is DKIM authenticated.

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.

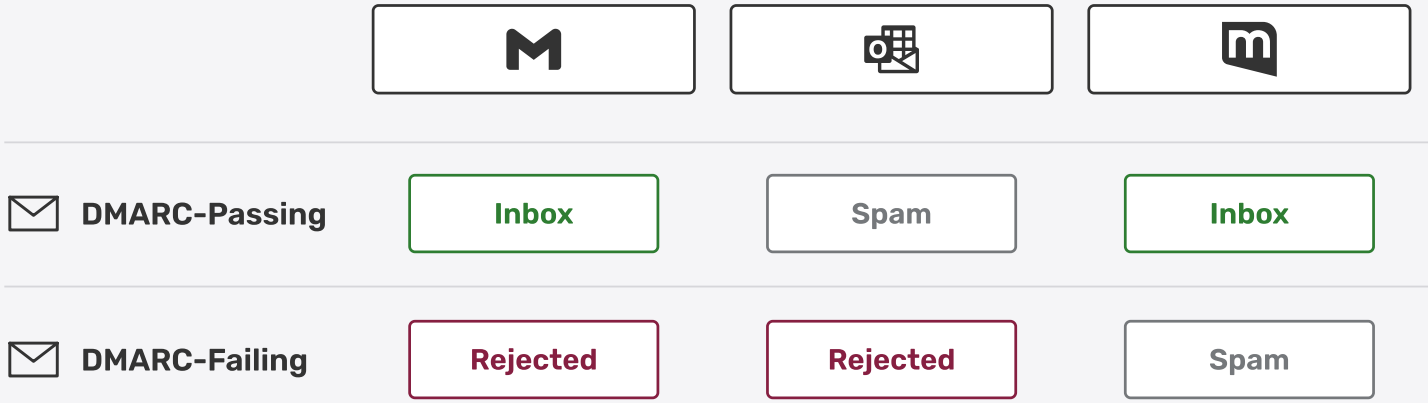
Split Alignment



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

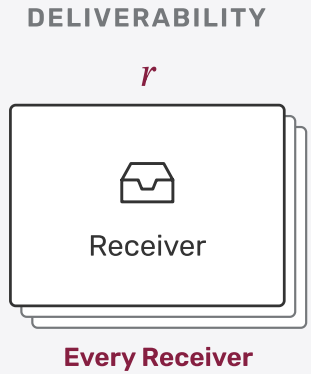
Evaluating Split Alignment

Evaluating Split Alignment



Evaluating Split Alignment

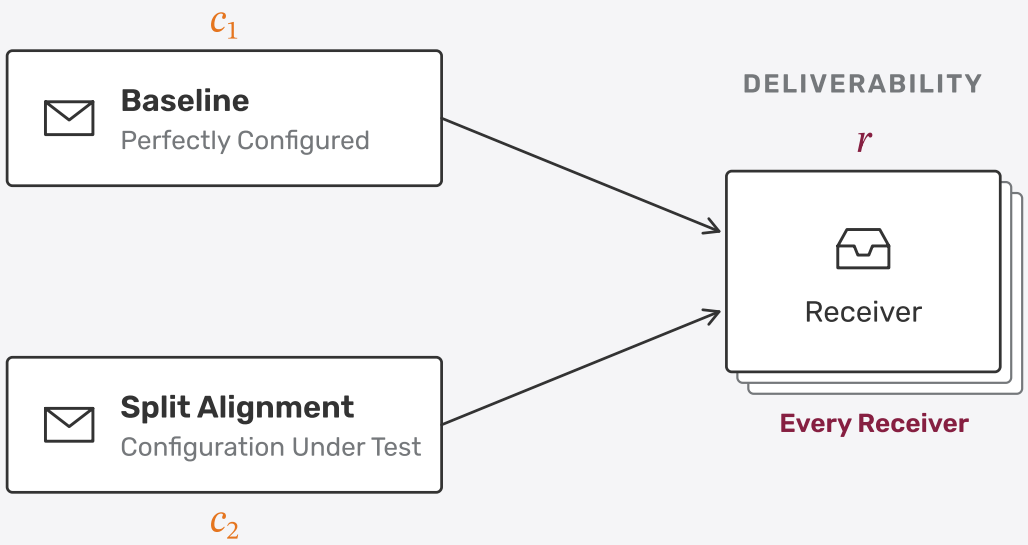
We evaluate deliverability through differential comparison within each receiver.



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

Evaluating Split Alignment

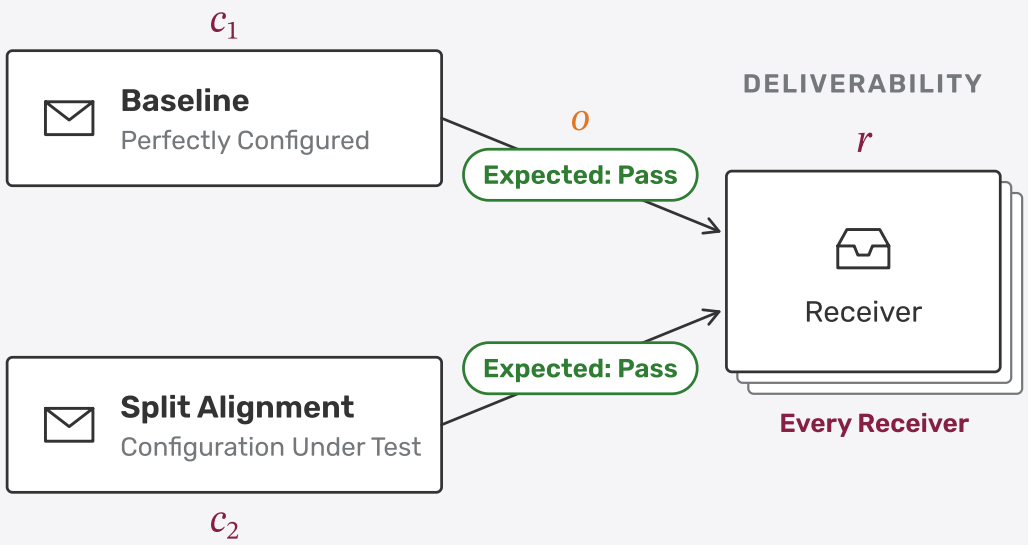
We evaluate deliverability through differential comparison within each receiver.



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

Evaluating Split Alignment

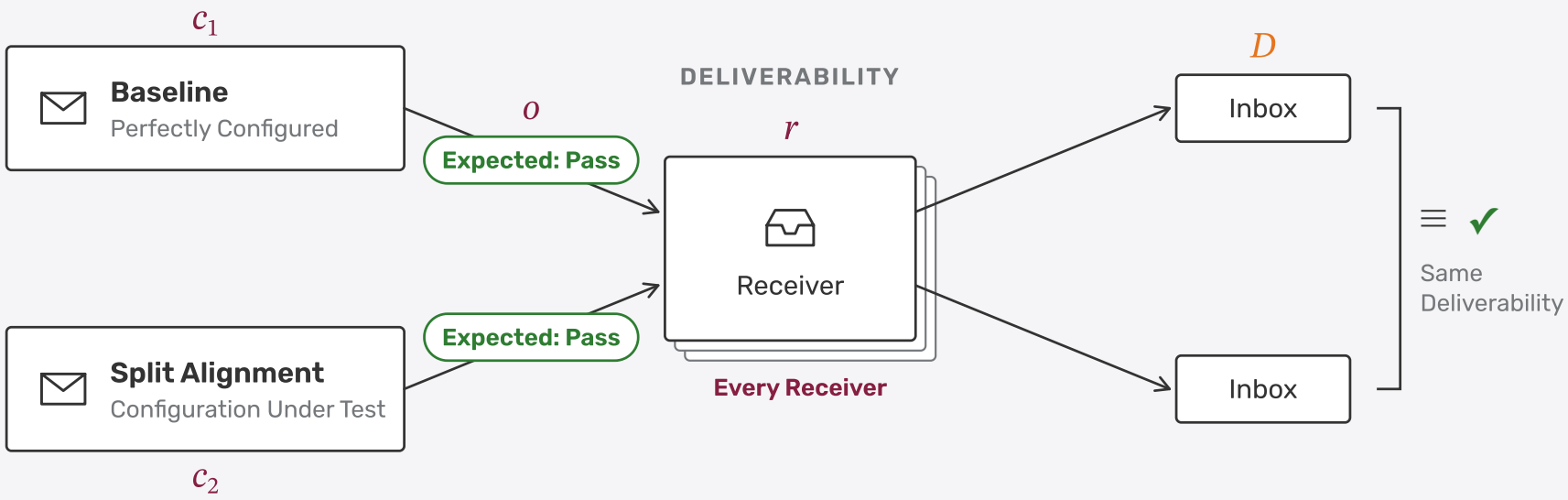
We evaluate deliverability through differential comparison within each receiver.



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

Evaluating Split Alignment

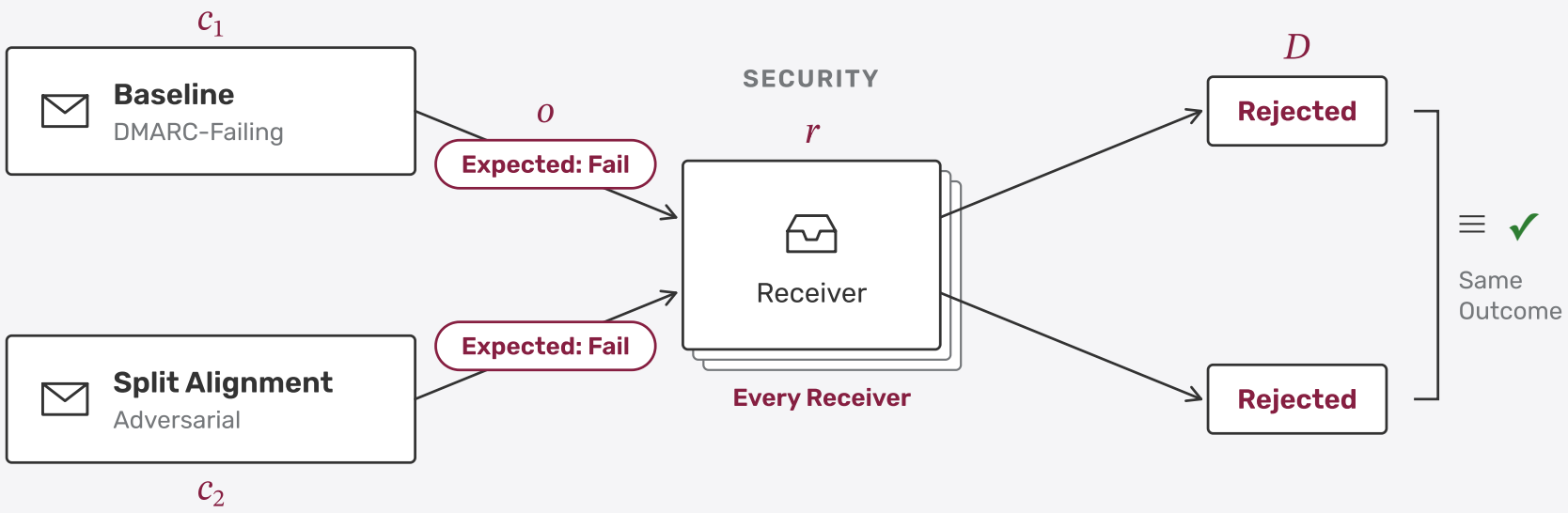
We evaluate deliverability through differential comparison within each receiver.



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

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

gmail.com
outlook.com
proton.me
yahoo.com
aol.com
zoho.com
naver.com
tuta.com
onet.pl
yandex.com
mailo.com
mail.com
inbox.lv
sapo.pt
seznam.cz

Evaluating Split Alignment

Visible Domain	Deliverability	
	Org.	Sub.
gmail.com	✓$_i$	✓$_i$
outlook.com	✓$_s$	✓$_s$
proton.me	✓$_i$	✓$_i$
yahoo.com	✓$_i$	✓$_i$
aol.com	✓$_i$	✓$_i$
zoho.com	✓$_i$	✓$_i$
naver.com	✓$_i$	✓$_i$
tuta.com	✓$_i$	✓$_i$
onet.pl	✓$_i$	✓$_i$
yandex.com	✓$_s$	✓$_s$
mailo.com	✓$_i$	✓$_i$
mail.com	✓$_i$	✓$_i$
inbox.lv	✓$_i$	✓$_i$
sapo.pt	✓$_i$	✓$_i$
seznam.cz	✓$_i$	✓$_i$

Evaluating Split Alignment

	Deliverability		Security	
Visible Domain	**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	✓$_i$	✓$_i$	▲$_s$ → ✸	✓$_b$

Evaluating Split Alignment

	Deliverability		Security	
Visible Domain	**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	✓$_i$	✓$_i$	▲$_s$ → ✸	✓$_b$

Evaluating Split Alignment

	Deliverability		Security	
Visible Domain	**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	✓$_i$	✓$_i$	▲$_s$ → ✸	✓$_b$

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	✓ $_i$	✓ $_i$	▲ $_i$ → ✓ $_s$	✓ $_s$
yah				
aol.c				
zoh				
nave				
tuta				
onet				
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	✓ $_i$	✓ $_i$	▲ $_s$ → ✸	✓ $_b$

> *"…what you observed is not a bug, but an intentional implementation decision by our team… This is a conscious choice aimed at improving overall deliverability…"*
>
> **— David Bořík, Seznam.cz**

Takeaways

All findings apply to DMARCbis [1].

[1] T. Herr and J. Levine, Eds., “Domain-Based Message Authentication, Reporting, and Conformance (DMARC),” RFC 9989, May 2026. rfc-editor.org/rfc/rfc9989

Takeaways



Retire SPF

SPF weaknesses remain widespread despite being well known, and they propagate up the protocol stack.

All findings apply to DMARCbis [1].

[1] T. Herr and J. Levine, Eds., “Domain-Based Message Authentication, Reporting, and Conformance (DMARC),” RFC 9989, May 2026. rfc-editor.org/rfc/rfc9989

Takeaways



Retire SPF

SPF weaknesses remain widespread despite being well known, and they propagate up the protocol stack.



Deny By Default

Default configuration remains the norm in the wild. DMARC's configuration should default to strict and enforcing.

All findings apply to DMARCbis [1].

[1] T. Herr and J. Levine, Eds., "Domain-Based Message Authentication, Reporting, and Conformance (DMARC)," RFC 9989, May 2026. rfc-editor.org/rfc/rfc9989

Takeaways



Retire SPF

SPF weaknesses remain widespread despite being well known, and they propagate up the protocol stack.



Deny By Default

Default configuration remains the norm in the wild. DMARC's configuration should default to strict and enforcing.



Design For Deliverability

Deliverability remains the primary goal for senders and receivers and should be part of the protocol design philosophy.

All findings apply to DMARCbis [1].

[1] T. Herr and J. Levine, Eds., "Domain-Based Message Authentication, Reporting, and Conformance (DMARC)," RFC 9989, May 2026. rfc-editor.org/rfc/rfc9989

Takeaways

Retire SPF

SPF weaknesses remain widespread despite being well known, and they propagate up the protocol stack.

Deny By Default

Default configuration remains the norm in the wild. DMARC's configuration should default to strict and enforcing.

Design For Deliverability

Deliverability remains the primary goal for senders and receivers and should be part of the protocol design philosophy.

WEBSITE

PAPER

All findings apply to DMARCbis [1].

[1] T. Herr and J. Levine, Eds., "Domain-Based Message Authentication, Reporting, and Conformance (DMARC)," RFC 9989, May 2026. rfc-editor.org/rfc/rfc9989