Domain-based Email Authentication:

SPF, DKIM, and DMARC

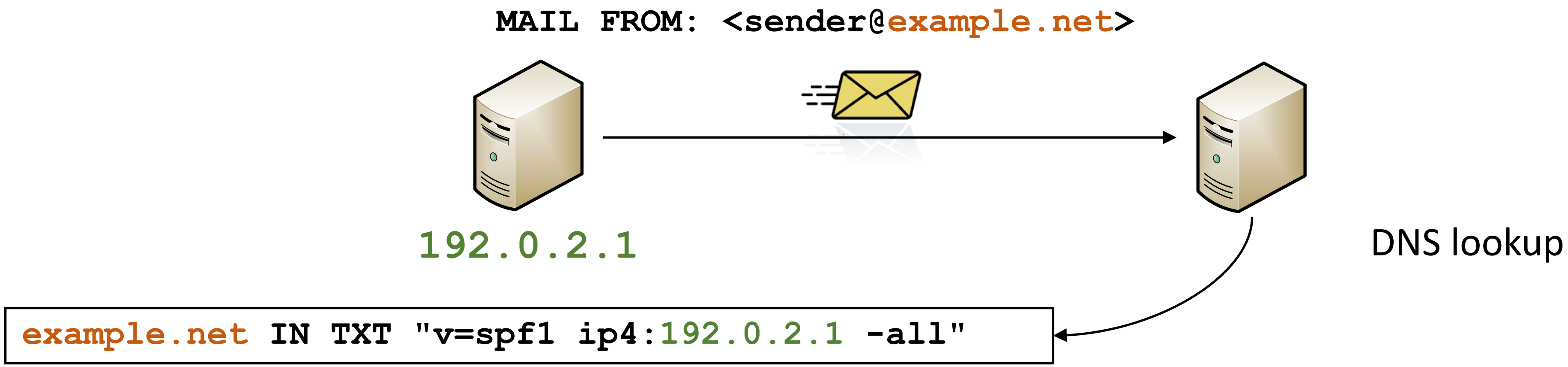
Matthäus Wander

2023-03-31

What is Email Authentication?

- Verifies the identity of the sender of an email message
- Purpose: Prevent email spoofing and phishing attacks
- **Domain-based** email authentication methods
  - SPF (Sender Policy Framework)
  - DKIM (DomainKeys Identified Mail)
  - DMARC (Domain-based Message Authentication, Reporting, and Conformance)
- Out of scope: address-based email authentication methods
  - S/MIME
  - OpenPGP

SPF (Sender Policy Framework)



```
MAIL FROM: <sender@example.net>
```

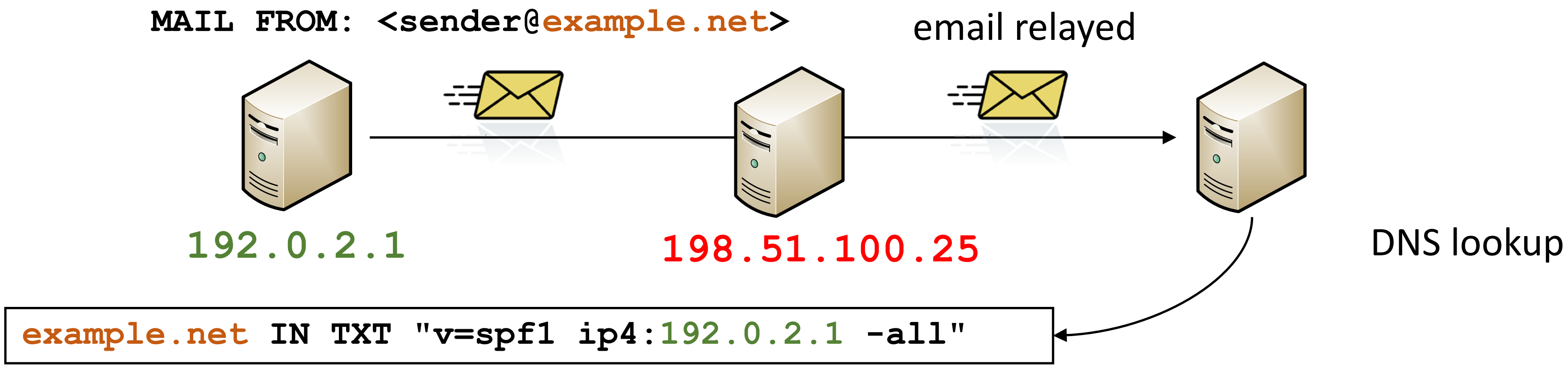
192.0.2.1

DNS lookup

```
example.net IN TXT "v=spf1 ip4:192.0.2.1 -all"
```

- Domain owner publishes IP addresses of authorized senders in DNS
- Receiving mail server looks up SPF record
- Compares sender IP address to authorized senders in SPF record

SPF is Incompatible with Email Relaying



`MAIL FROM: <sender@example.net>`

email relayed

192.0.2.1

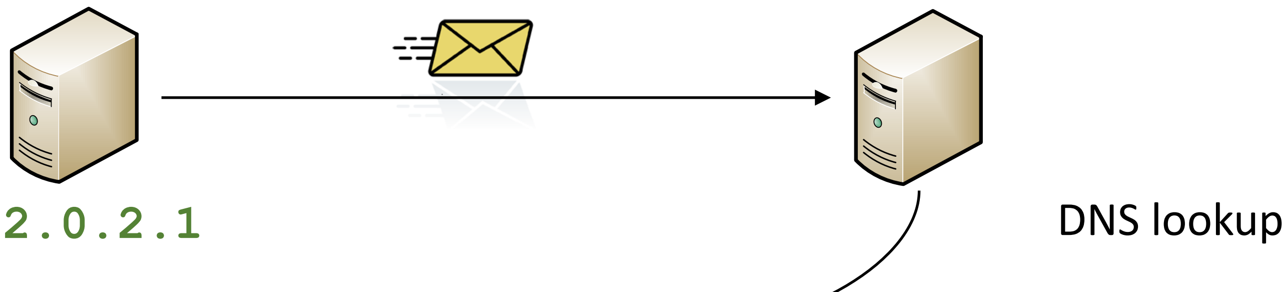
198.51.100.25

DNS lookup

```
example.net IN TXT "v=spf1 ip4:192.0.2.1 -all"
```

- Does not support email relaying: IP address mismatch
  - e.g. alias@cryptool.org relaying emails to personal mailbox
- Same problem with mailing lists

SPF Protects the Wrong From Address

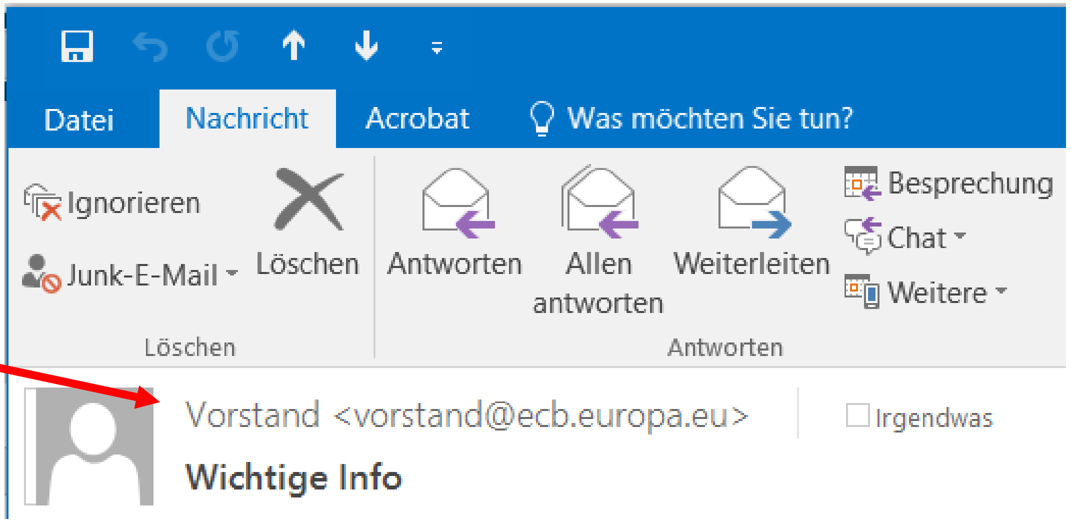


```
example.net IN TXT "v=spf1 ip4:192.0.2.1 -all"
```

used for SPF check

```
MAIL FROM: <attacker@example.net>
...
DATA
From: Vorstand <vorstand@ecb.europa.eu>
Subject: Wichtige Info
```

shown in mail client

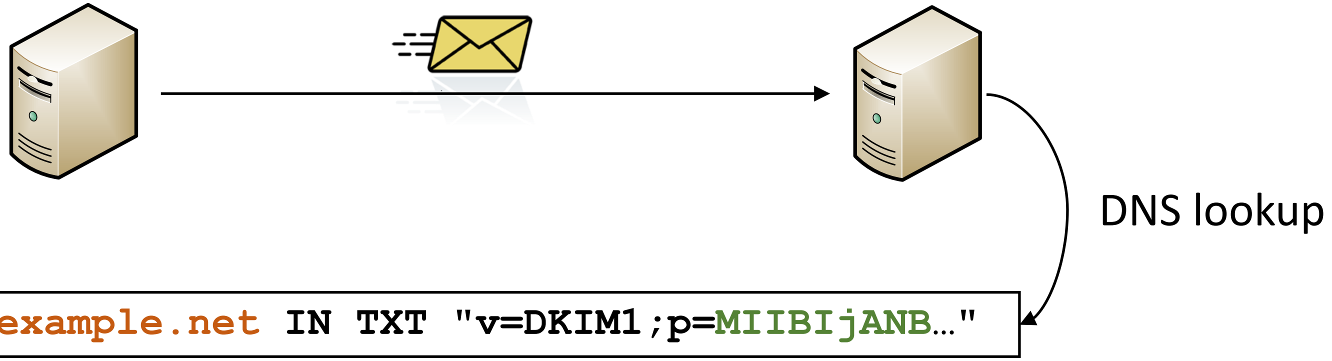


Vorstand <vorstand@ecb.europa.eu>

Wichtige Info

DKIM (DomainKeys Identified Mail)

```
DKIM-Signature: d=example.net; s=selector; b=W7W1XjN/5yRz…
```



```
selector._domainkey.example.net IN TXT "v=DKIM1;p=MIIBIjANB…"
```

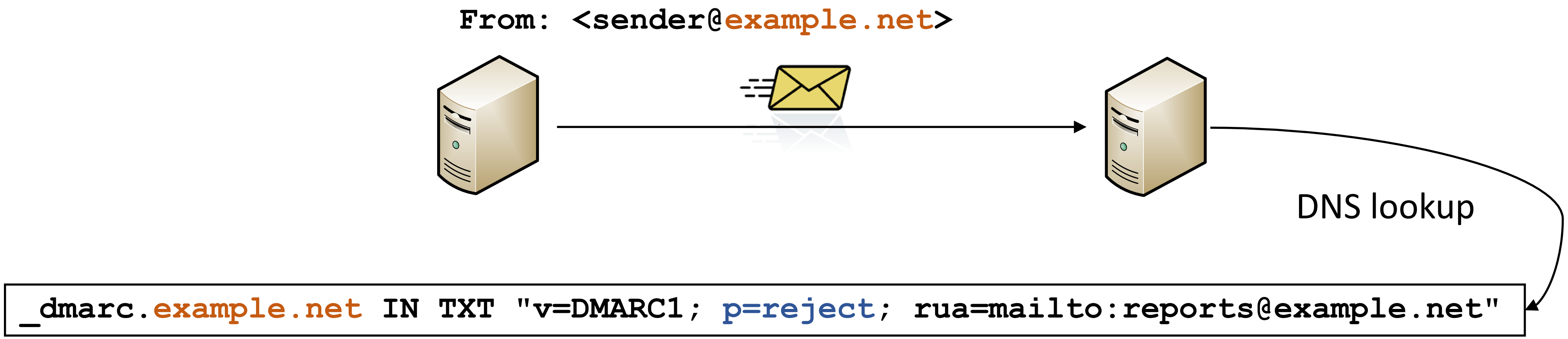
- Domain owner publishes public key in DNS
  - … uses private key to add a digital signature to email
- Receiving mail server looks up public key from DKIM record
  - … verifies DKIM-Signature with authorized public key

Common Problems with DKIM

- DKIM supports email relaying
  - … but only if the message remains unchanged
  - Mailing lists regularly break DKIM-Signature
- DKIM has no default policy
  - No DKIM-Signature: sender does not use DKIM signing?
  - No DKIM-Signature: attacker stripped off DKIM-Signature?
- DKIM does not check whether header From aligns with DKIM domain

```
DKIM-Signature: d=example.net; s=selector; b=W7W1XjN/5yRz…
From: Vorstand <vorstand@ecb.europa.eu>
Subject: Wichtige Info
```

DMARC Adds a Domain Authentication Policy



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

- **D**omain-based **M**essage **A**uthentication, **R**eporting, and **C**onformance
- DMARC builts on top of SPF and DKIM
- Domain owner publishes policy how to handle authentication failures
  - p=none, p=quarantine, or p=reject

DMARC Requires Identifier Alignment

`From: <sender@example.net>`

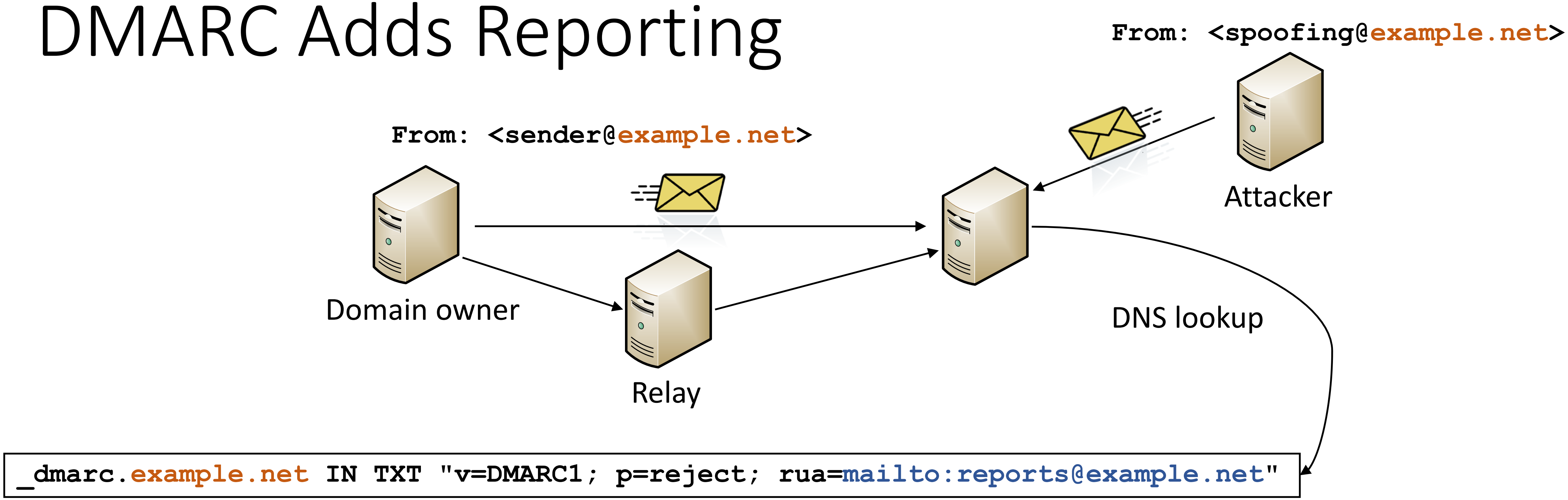
- SPF: Envelope-From domain must be aligned with header From
- DKIM: d= domain must be aligned with header From

```
MAIL FROM: <sender@example.net>
...
DATA
DKIM-Signature: d=example.net; s=selector; b=W7W1XjN/5yRz…
From: <sender@example.net>
Subject: Wichtige Info
```

Envelope-From aligned?

DKIM d= domain aligned?

DMARC Adds Reporting



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

- Receiving mail server sends aggregate report to domain owner
- Reports allow domain owner to monitor DMARC conformance
  - … SPF/DKIM configuration complete and effective?

Demo