PCI Security Standards Council®

2025 EUROPE COMMUNITY MEETING

2025 EUROPE COMMUNITY MEETING

Best Practices for Anti-Phishing Mechanisms

(PCI DSS v4.0 Req 5.4)

PCI Security Standards Council

Vui Huang Tea

Cyber Security Infrastructure Engineer

Swedbank

PCI Security Standards Council

PCI DSS v4.0.1 Section 5.4.1

5.4 Anti-phishing mechanisms protect users against phishing attacks.

5.4.1 Processes & automated mechanisms are in place to detect & protect personnel against phishing attacks.

- When developing anti-phishing controls, entities are encouraged to consider a combination of approaches. For example, using anti-spoofing controls such as
  - **DMARC**: Domain-based Message Authentication, Reporting & Conformance
  - **SPF**: Sender Policy Framework
  - **DKIM**: Domain Keys Identified Mail

  will help stop phishers from spoofing the entity's domain and impersonating personnel

Developing Anti-Phishing Controls

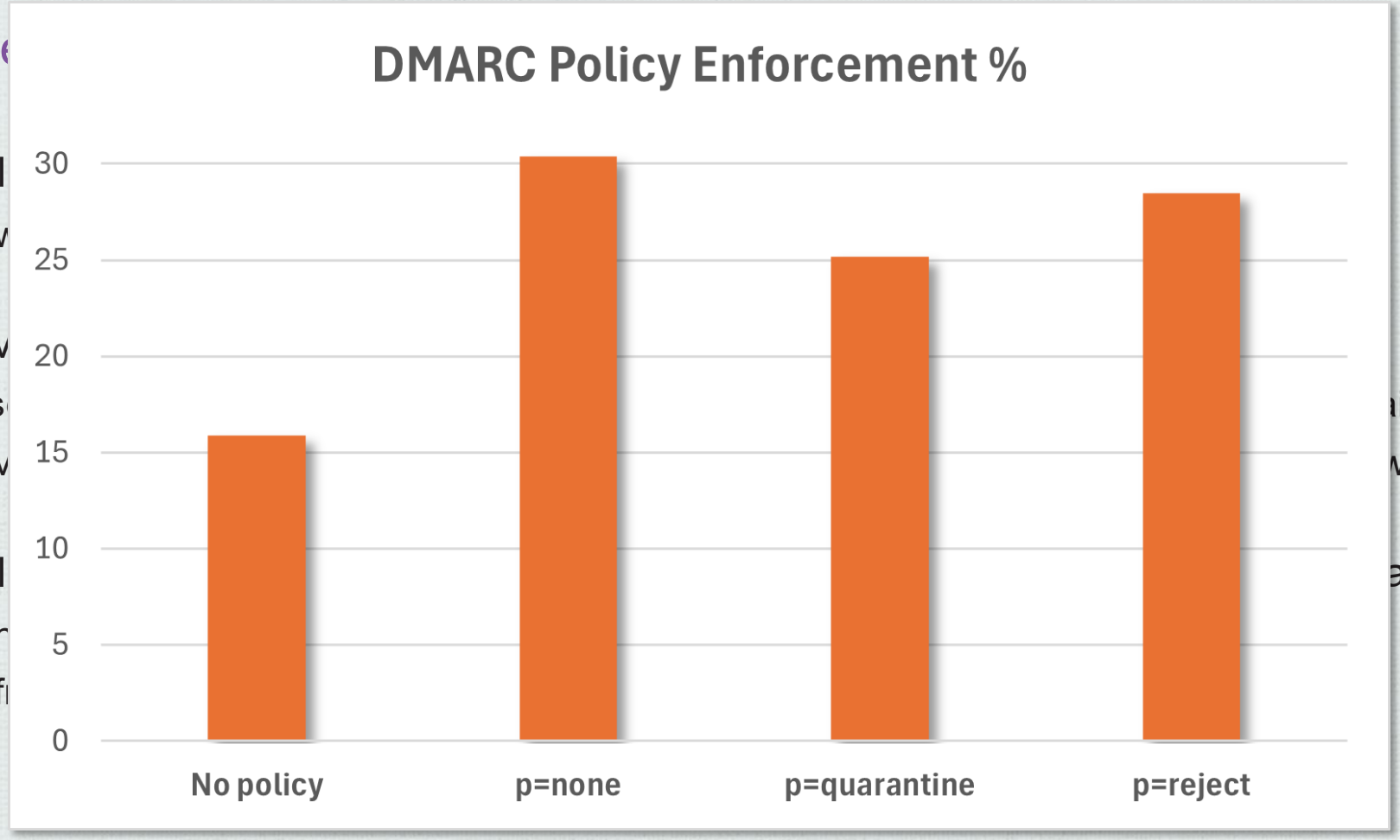
General sequence taken by Email domain owners

1. Define & publish **SPF** (Sender Policy Framework) policy
   - To specify which senders are permitted to use an organization's domain name
2. Define & activate **DKIM** (Domain Keys Identified Mail)
   - Senders use their DKIM signing key to create & attach cryptographic signature on out-going emails
   - Receivers verify the DKIM signature to assert that the in-coming email has not changed since it was signed
3. Define & publish **DMARC** (Domain-based Message Authentication, Reporting & Conformance) policy
   - To specify how receivers should handle suspicious emails (failing **SPF**/**DKIM**) using their domain name
   - Beginning from policy levels 'None' to ' Quarantine' to 'Reject'

Developing Anti-Phishing Controls

General seque

1. Define & publ
   - To specify v
2. Define & activ
   - Senders us
   - Receivers v
3. Define & publ
   - To specify h
   - Beginning f



ils

was signed

ance) policy

name

PCI Security Standards Council

Data Sources

- **SPF** (Sender Policy Framework)
  - Based on ~3,000 configurations (~2,000 email domains and ~1,000 1st level 'includes')
  - PCI validated service providers / participating organizations & Financial institutions in Scandinavia / Baltics
- **DKIM** (Domain Keys Identified Mail)
  - Based on ~8,000 configurations
  - Finance-related organizations in Scandinavia / Baltics
- **DMARC** (Domain-based Message Authentication, Reporting & Conformance)
  - Based on ~2,000 configurations
  - PCI validated service providers / participating organizations & Financial institutions in Scandinavia / Baltics

SPF

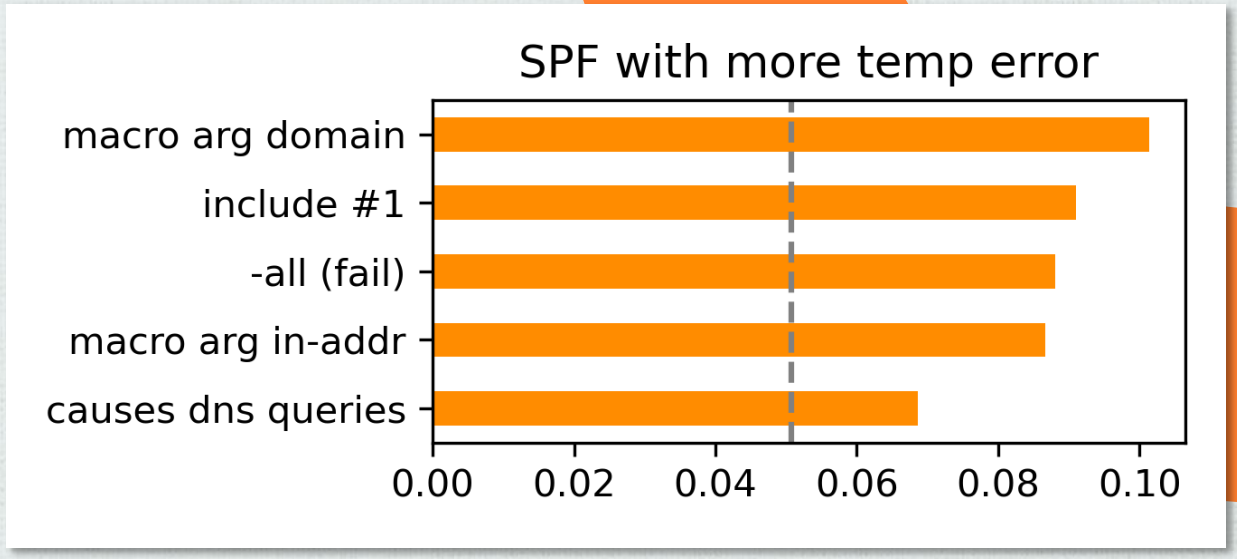
Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, V1
RFC 7208

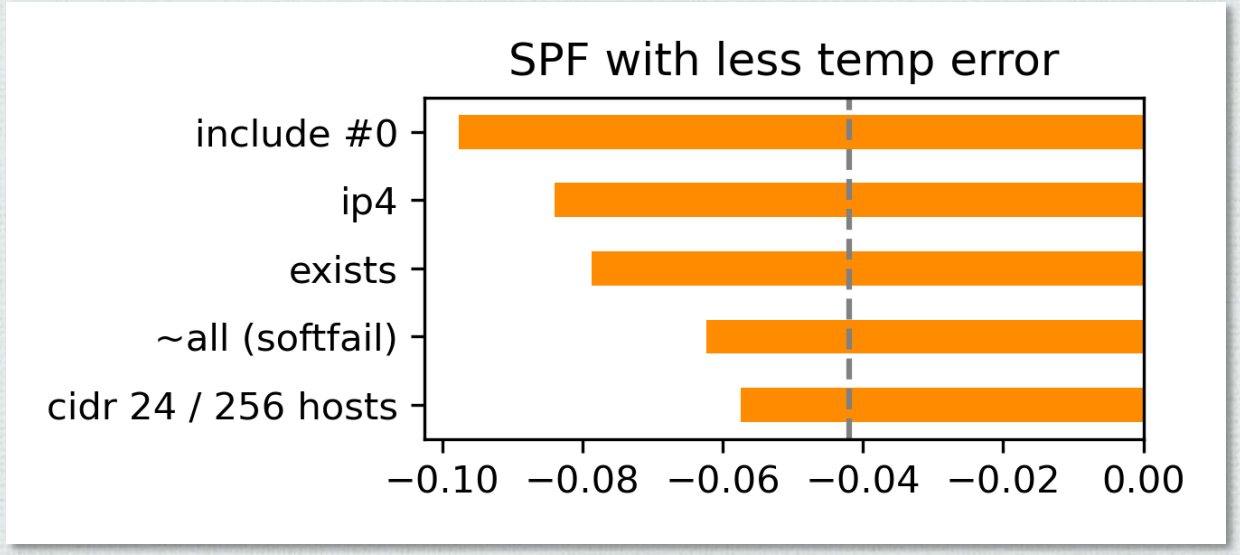
PCI Security Standards Council

SPF Temp Error

Occurs when the SPF verifier encounters a transient error while performing the SPF check

- Result of: DNS lookup time-out, SPF evaluation exceeded 20 sec etc.
- Side effects on SPF verifier: Wastes computation effort, uses excessive memory, triggers bugs, exhaust DNS resources
- If a receiver is configured to accept mail with an SPF result of "temperror", this might result in mail that would otherwise have been rejected due to an SPF "fail" result being accepted





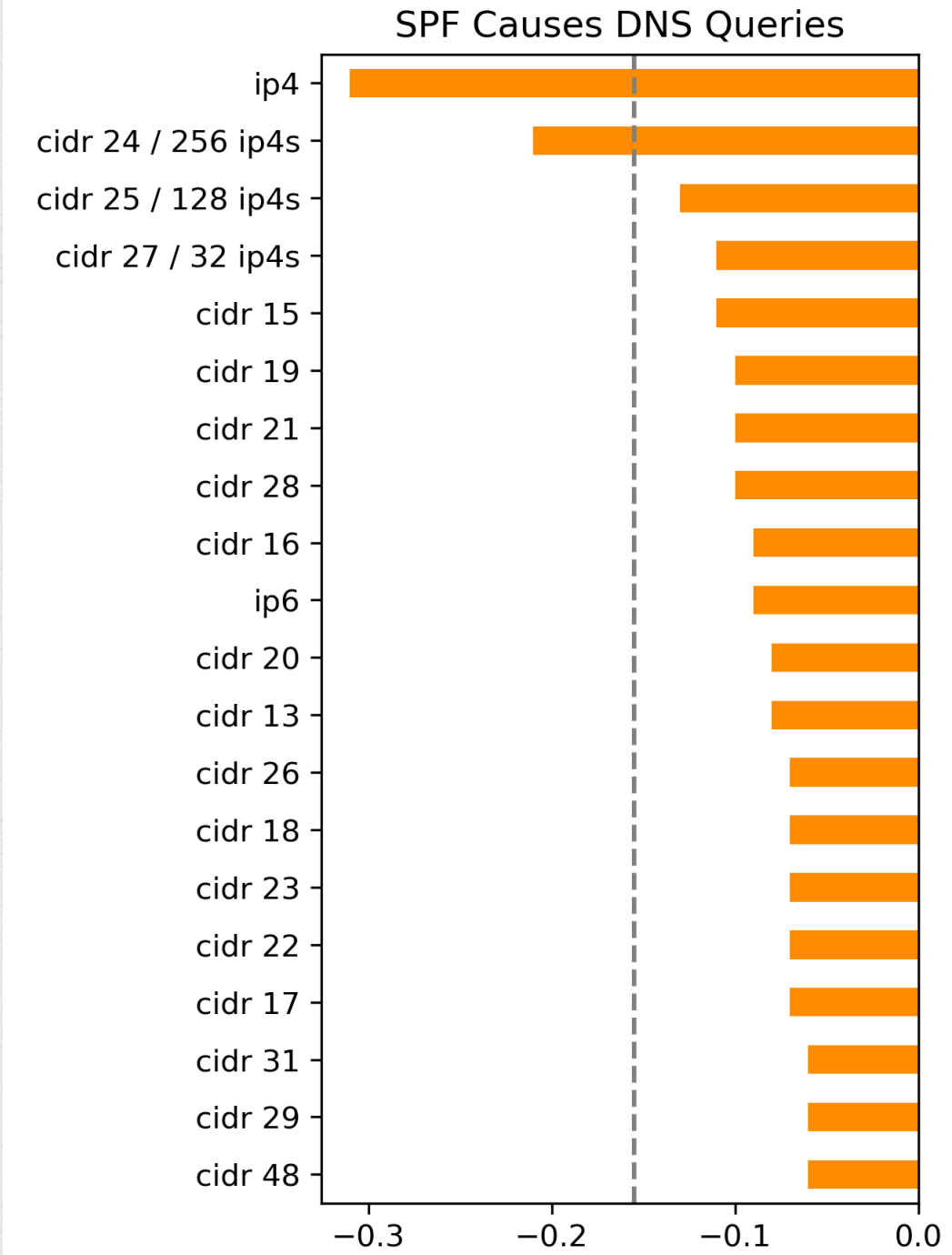
PCI Security Standards Council

SPF Not Causing DNS Queries

SPF mechanisms ‘ip4’ & ‘ip6’ are less resource-intensive & do not query the DNS

Notable details:

- IPv4 (32-bit address) are more commonly used than IPv6 (128-bit address)
- CIDR (Classless Inter-Domain Routing) specifies the range of IPs to check. Common values are 24 & 25 (256 & 128 IPs)

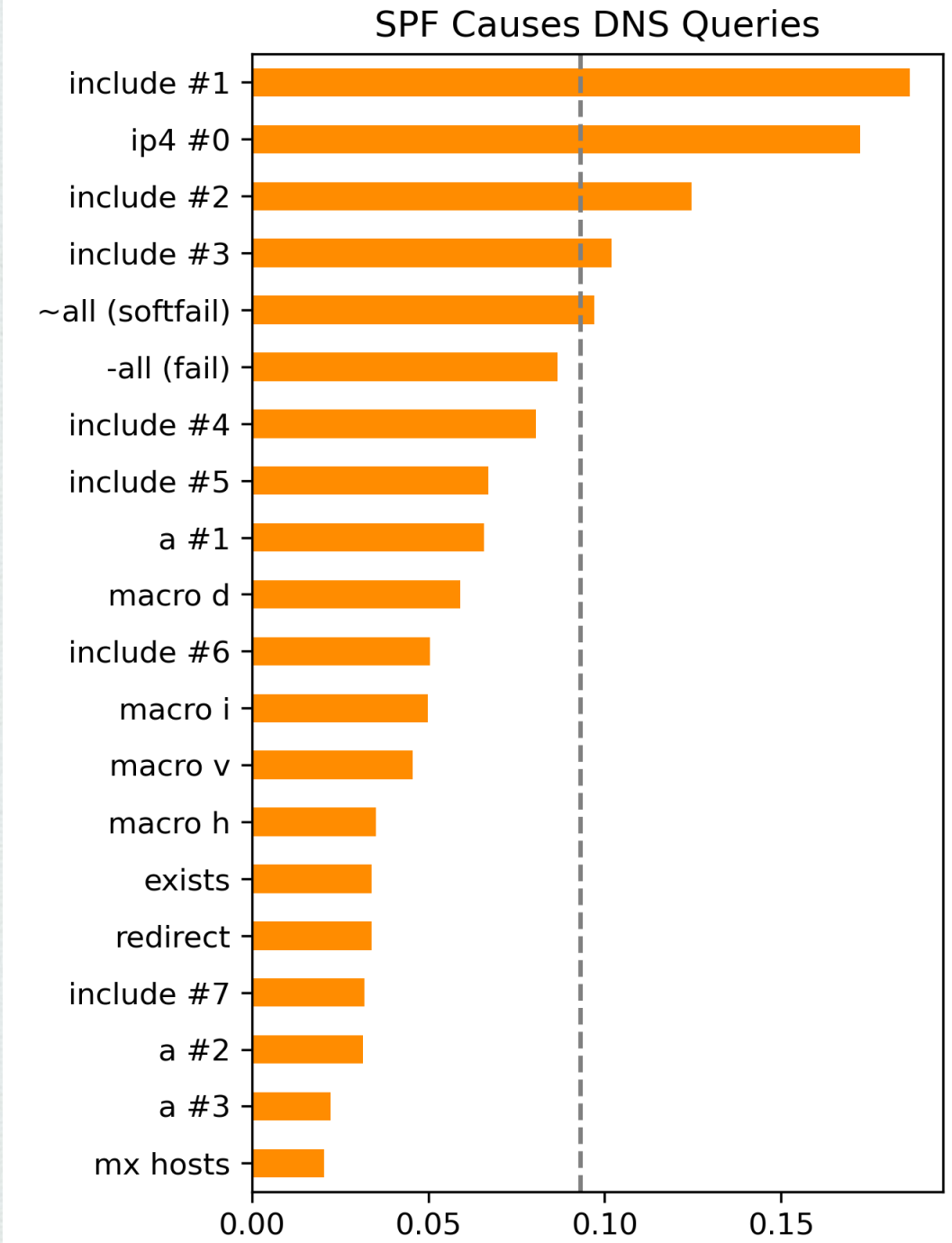


SPF Causing DNS Queries

Inappropriate use of SPF parameters could create unreasonable load on the DNS

Notable details:

- The "include" mechanism makes it possible for one domain to designate multiple administratively independent domains. Usually 1, 2 and 3 is used
- Qualifier for explicit default ‘all’: ~/- (‘softfail’ = probably not authorized / ‘fail’ = not authorized)
- Common Macros (character sequences to be dynamically replaced by message / connection details): d, i, v, h



Key Points

Typos

SPF is expressed as text in a DNS record. Text strings are susceptible to typographical error. E.g. spelling mistakes, incorrect punctuations, etc, These will cause the SPF to be ignored by the receiver

Parameters & Values

SPF is composed of numerous parameters referred to as 'mechanisms' & 'modifiers'. It is vital to use the correct sets with the corresponding values for each scenario

DNS Usage Considerations

SPF relies heavily on DNS. Minimize DNS usage by choosing parameters that require less DNS information and by placing lower-cost mechanisms earlier in the SPF record, e.g. ip/a/mx

Macros

Macros are not commonly used in the PCI community. Security consideration: Macros allows senders to inject hostile or unexpected content into receiver DNS queries

DKIM

DomainKeys Identified Mail (DKIM) Signatures, RFC 6376

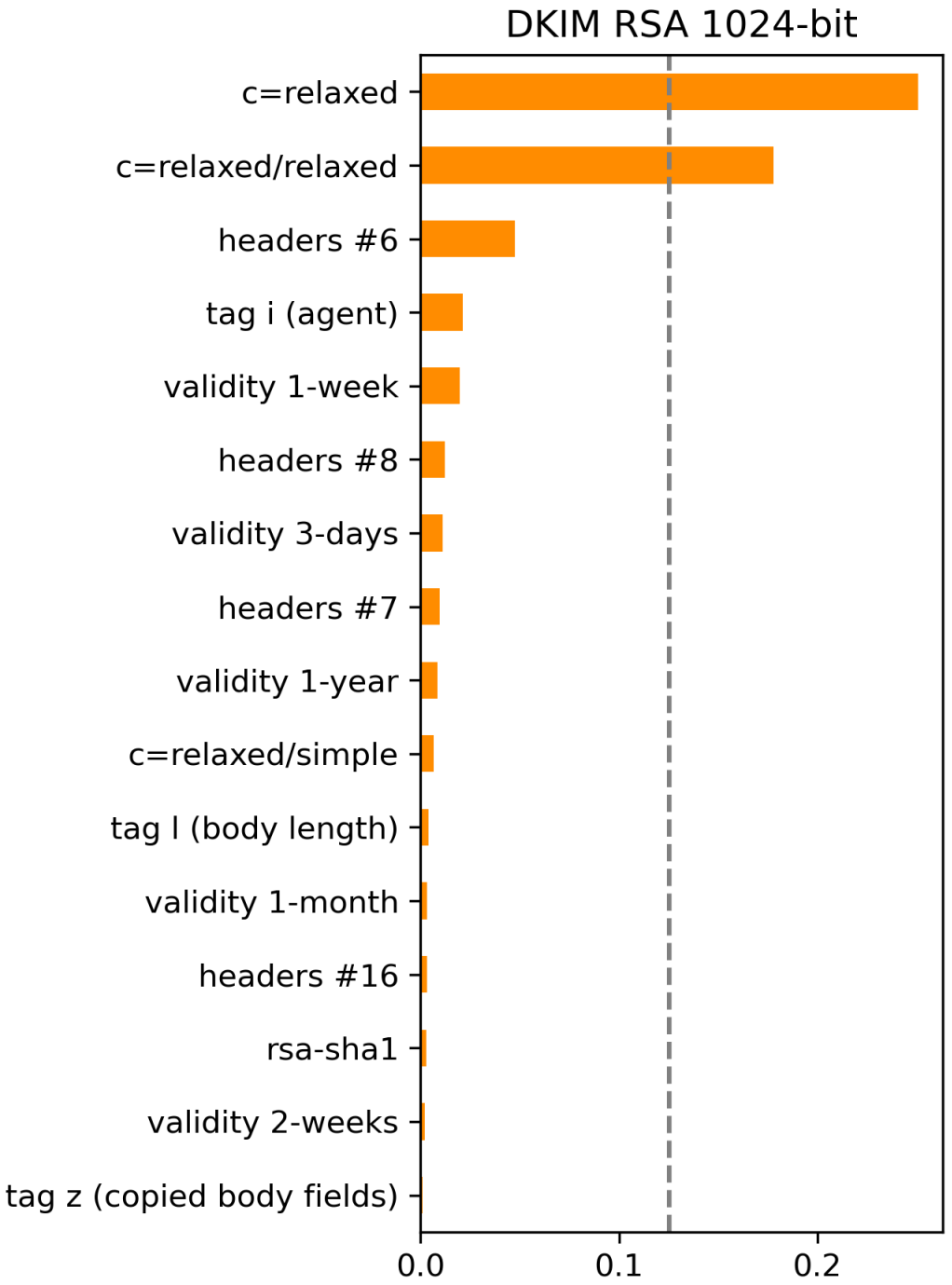
PCI Security Standards Council

DKIM Signing Key RSA 1024 bits

RSA-based DKIM signing keys smaller than 1024 bits are subject to off-line attacks

Notable details:

- Header & body canonicalization algorithms: c=relaxed, c=relaxed/relaxed (‘simple’ = no modification & ’relaxed’ = modifications)
- Number of signed header fields: 6, 8, 7
- Signature validity (expiration - timestamp): 1 week, 3 days, 1 year
- Signing algorithm: sha-256, sha-1 (minority)
- Signature header field tags: i (agent), l (body length) & z (copied body fields)

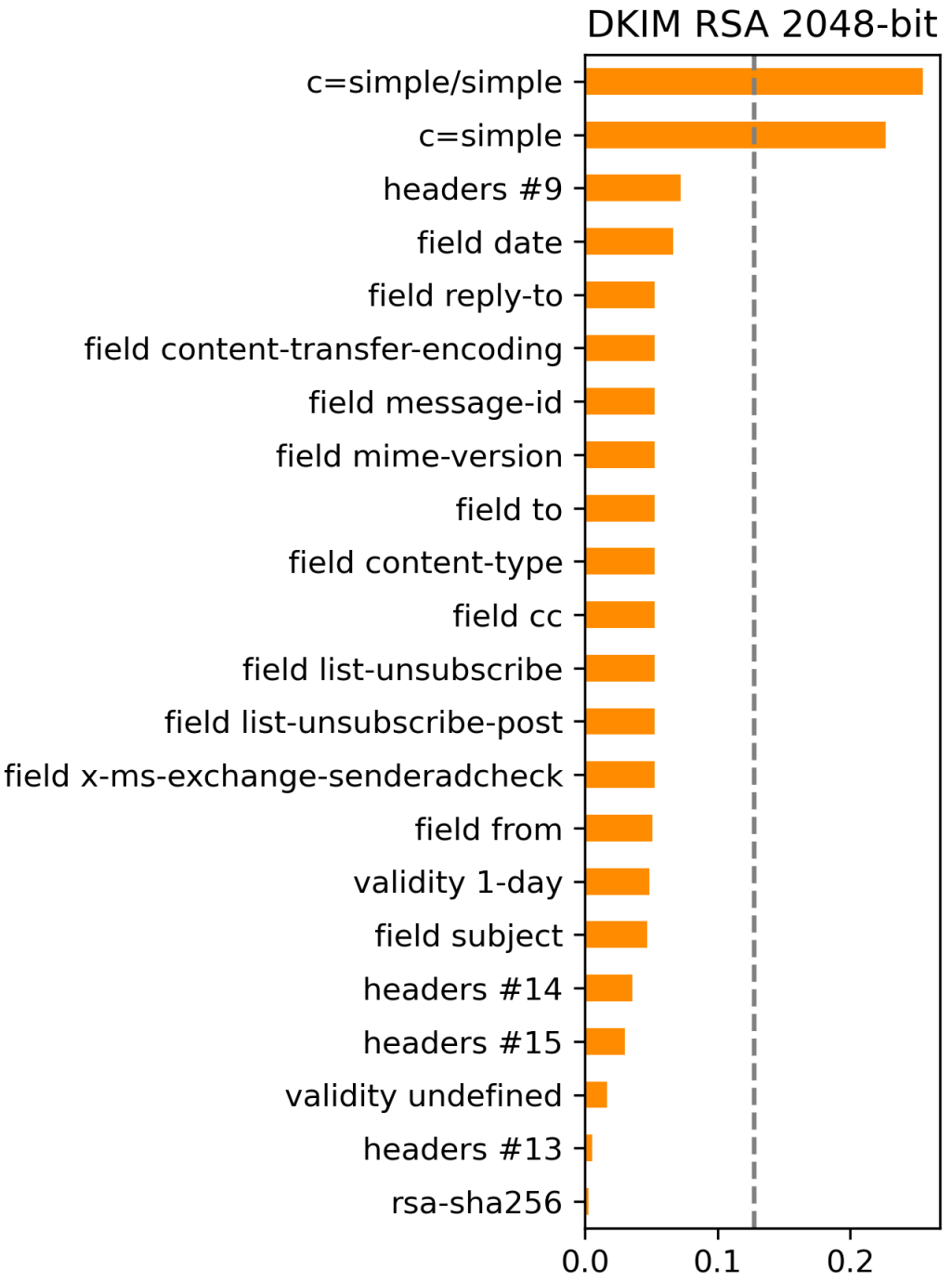


DKIM Signing Key RSA 2048 bits

Larger DKIM signing keys are more secure but impose higher CPU costs to verify & sign emails

Notable details:

- Header & body canonicalization algorithms: c=simple, c=simple/simple (‘simple’ = no modification & ’relaxed’ = modifications)
- Number of signed header fields: 9, 14, 15
- Signature validity (expiration - timestamp): 1 day, undefined
- Signing algorithm: sha-256 (only)

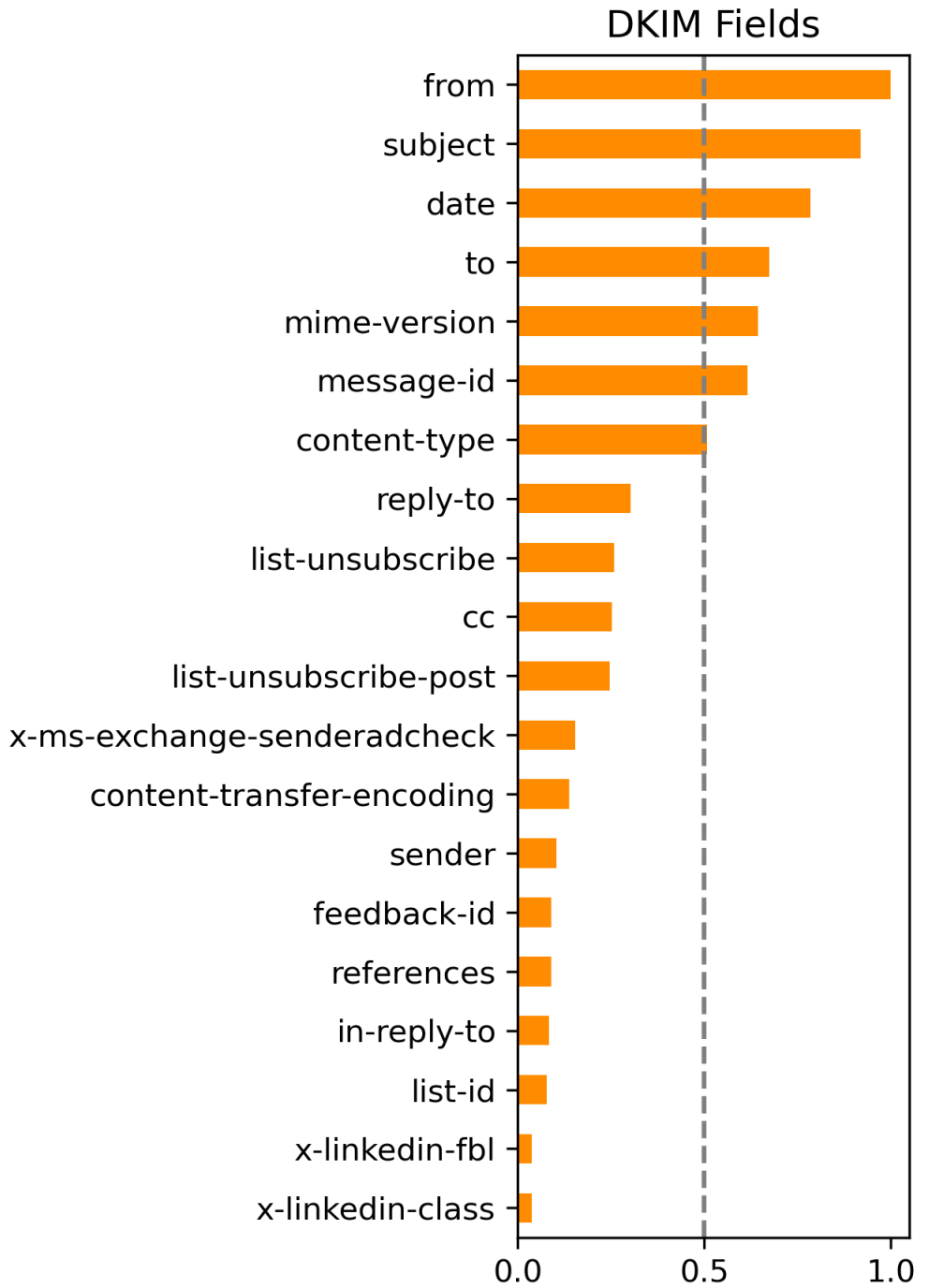


DKIM Signed Header Fields

Basic rule for choosing fields is to select fields that constitute the "core" of the message content

Common examples of fields with addresses and fields with textual content related to the body are:

- From (REQUIRED; see Section 5.4)
- Reply-To
- Subject
- Date
- To, Cc
- Resent-Date, Resent-From, Resent-To, Resent-Cc
- In-Reply-To, References
- List-Id, List-Help, List-Unsubscribe, List-Subscribe, List-Post, List-Owner, List-Archive



Key Points

Simple Key Management

DKIM does not use digital certificates. The Mail Receivers (‘verifiers’) retrieve the Mail Sender’s (‘signers’) public verification key from a DNS

Key Sizes

Signing keys smaller than 1024 bits are subject to off-line attacks. However, larger keys impose higher CPU costs to verify and sign email

Signed Headers

Basic rule is to select header fields that constitute the ‘core’ of the message content. Hence, any replay attack will have to include these in order to have the signature succeed

Head/Body Canonicalization

Signers should choose email canonicalization algorithms (simple/relaxed) based on the types of emails they process & their aversion to risk.

DMARC

Domain-based Message Authentication, Reporting, and Conformance (DMARC)
RFC 7489 ***None > Quarantine > Reject***

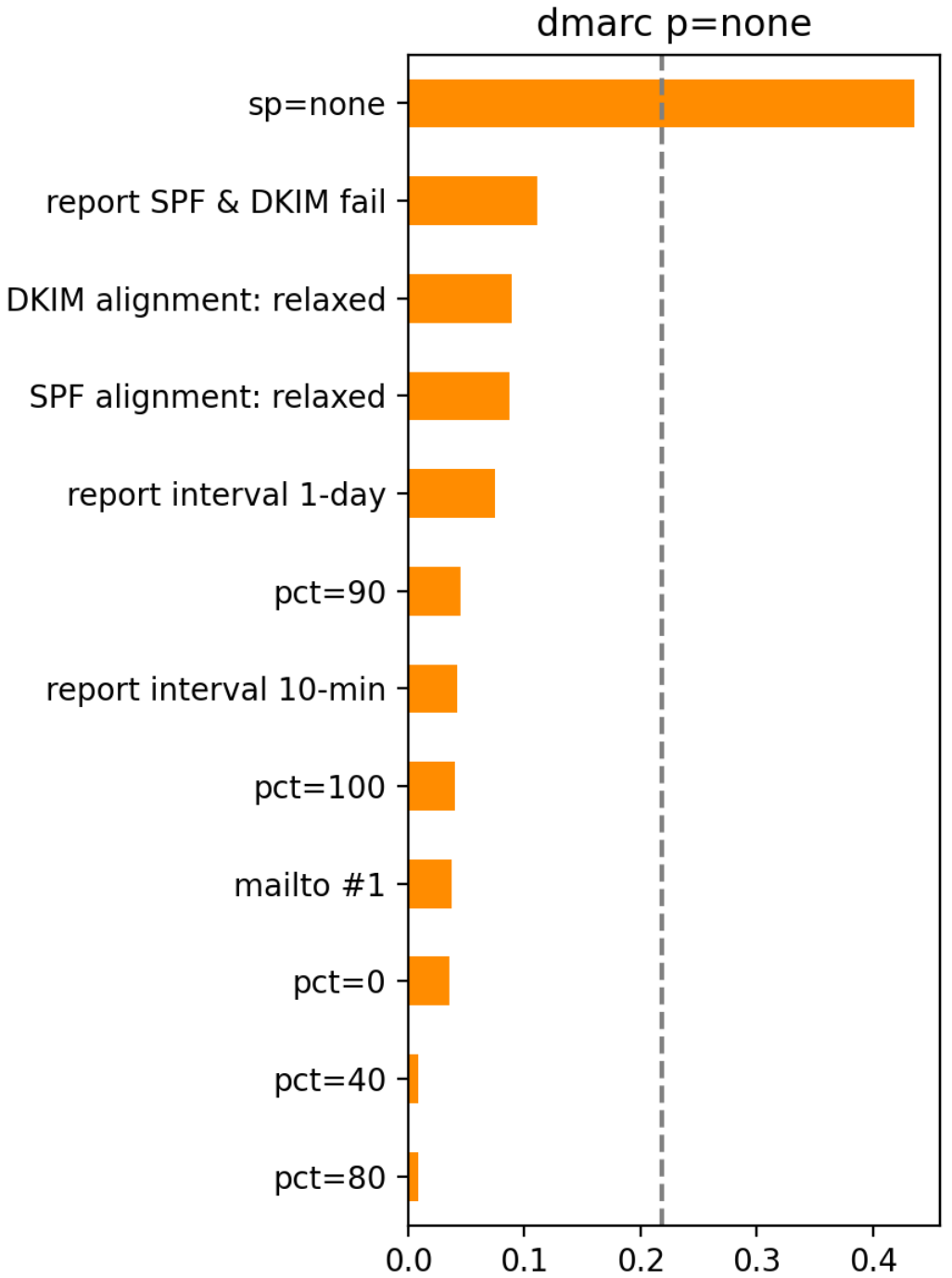
PCI Security Standards Council

DMARC Policy = None

Email domain owner requests no specific action be taken regarding delivery of messages

Notable details:

- Policy for all subdomains: None
- Report criteria: When both SPF & DKIM fail
- SPF & DKIM alignments: relaxed (‘strict’ = exact FQDN match & ’relaxed’ = otherwise)
- Report interval: 1 day, 10 mins
- Emails to apply policy on: 90%, 100%, 0%

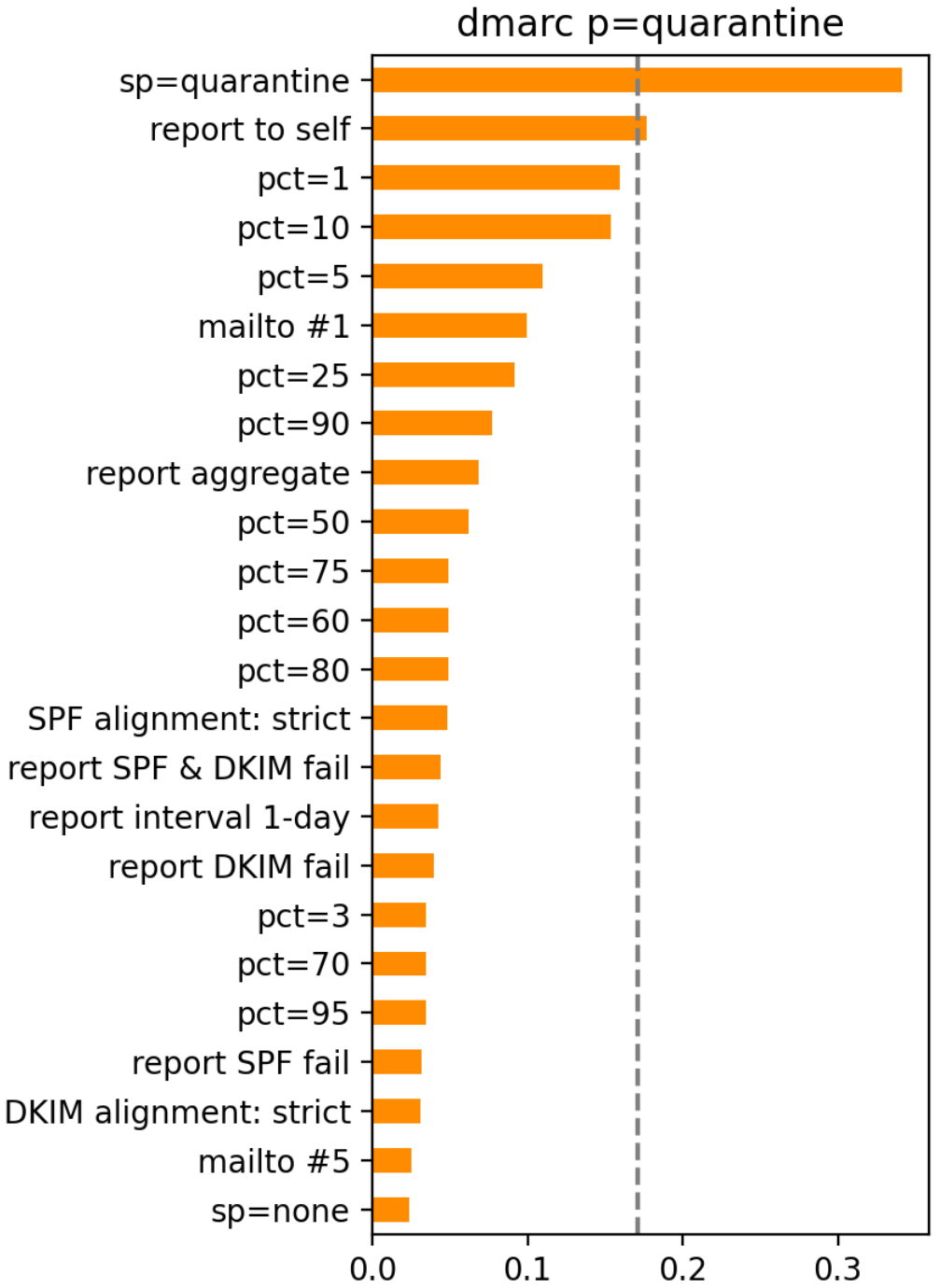


DMARC Policy = Quarantine

Email domain owner wishes to have email that fails the checks to be treated by as suspicious

Notable details:

- Policy for subdomains: Quarantine, None
- Report criteria: When both SPF & DKIM fail, DKIM fail, SPF fail
- SPF & DKIM alignments: strict (‘strict’ = exact FQDN match & ’relaxed’ = otherwise)
- Report interval: 1 day
- Emails to apply policy on: 1%, 10%, 5%
- Report type: aggregate (to self)

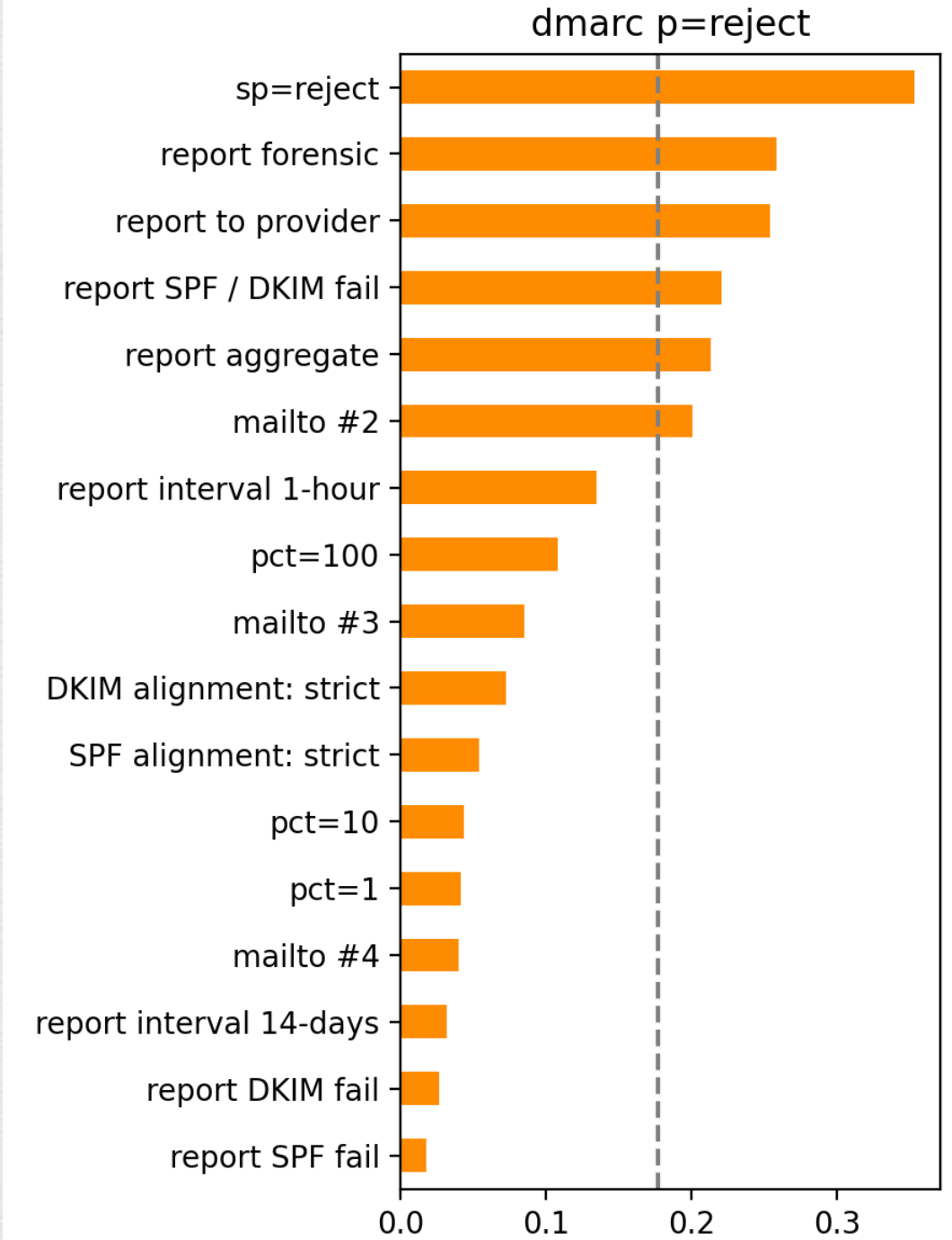


DMARC Policy = Reject

Email domain owner wishes for Mail Receivers to reject email that fails the checks

Notable details:

- Policy for subdomains: Reject
- Report criteria: When either SPF or DKIM fail, DKIM fail, SPF fail
- SPF & DKIM alignments: strict (‘strict’ = exact FQDN match & ’relaxed’ = otherwise)
- Report interval: 1 hour, 14 days
- Emails to apply policy on: 100%, 10%, 1%
- Report type: forensic, aggregate (to provider)



DMARC Report

Request Sending of Aggregate (RUA) / Forensic (RUF) Reports

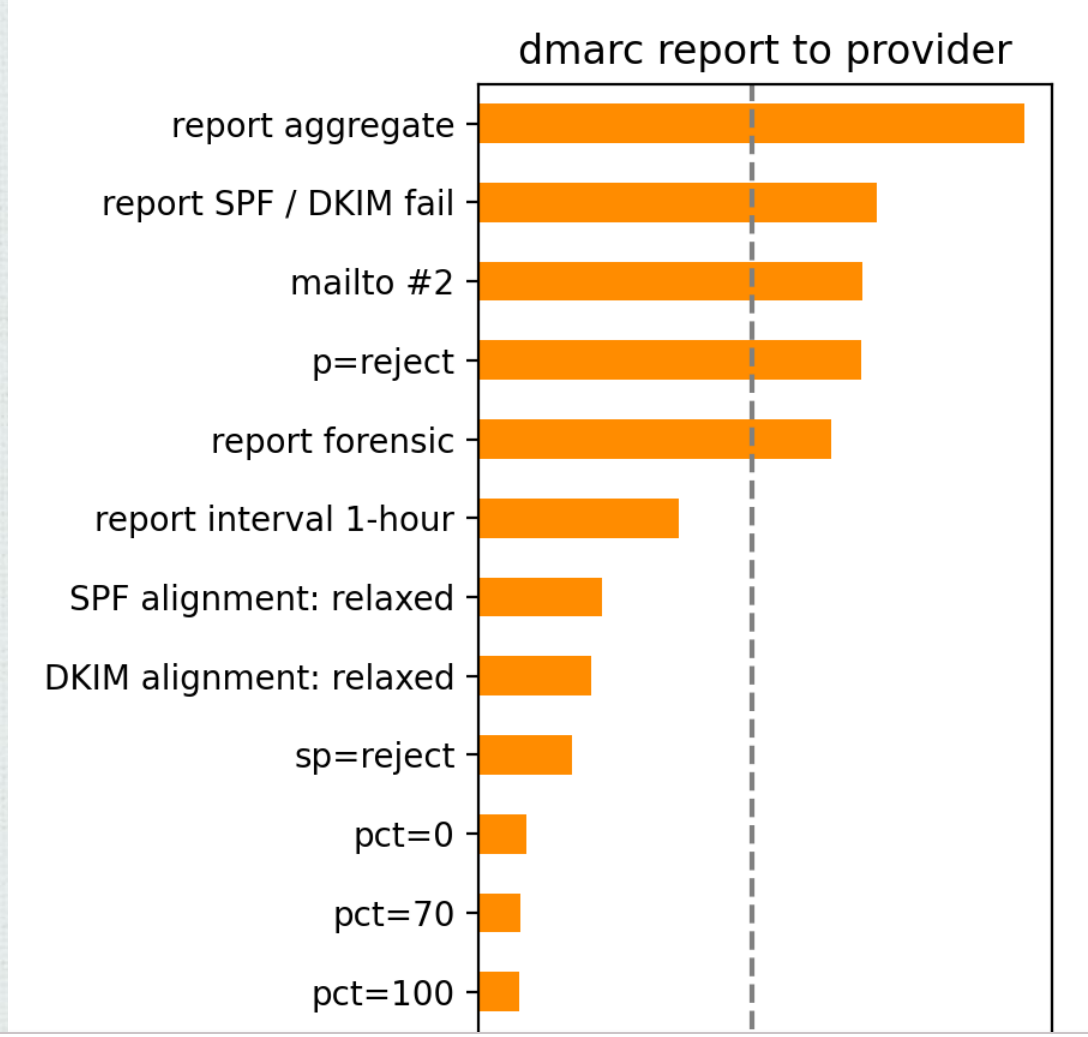
PCI Security Standards Council

Send Reports to Providers

Instruct receivers when to generate & send aggregate & message-specific info

Notable details:

- Policy for self: Reject
- Policy for subdomains: Reject
- Report criteria: When either SPF or DKIM fail
- SPF & DKIM alignments: 'relaxed' ('strict' = exact FQDN match & 'relaxed' = otherwise)
- Report interval: 1 hour
- Emails to apply policy on: 0%, 70%, 100%
- Report type: aggregate, forensic



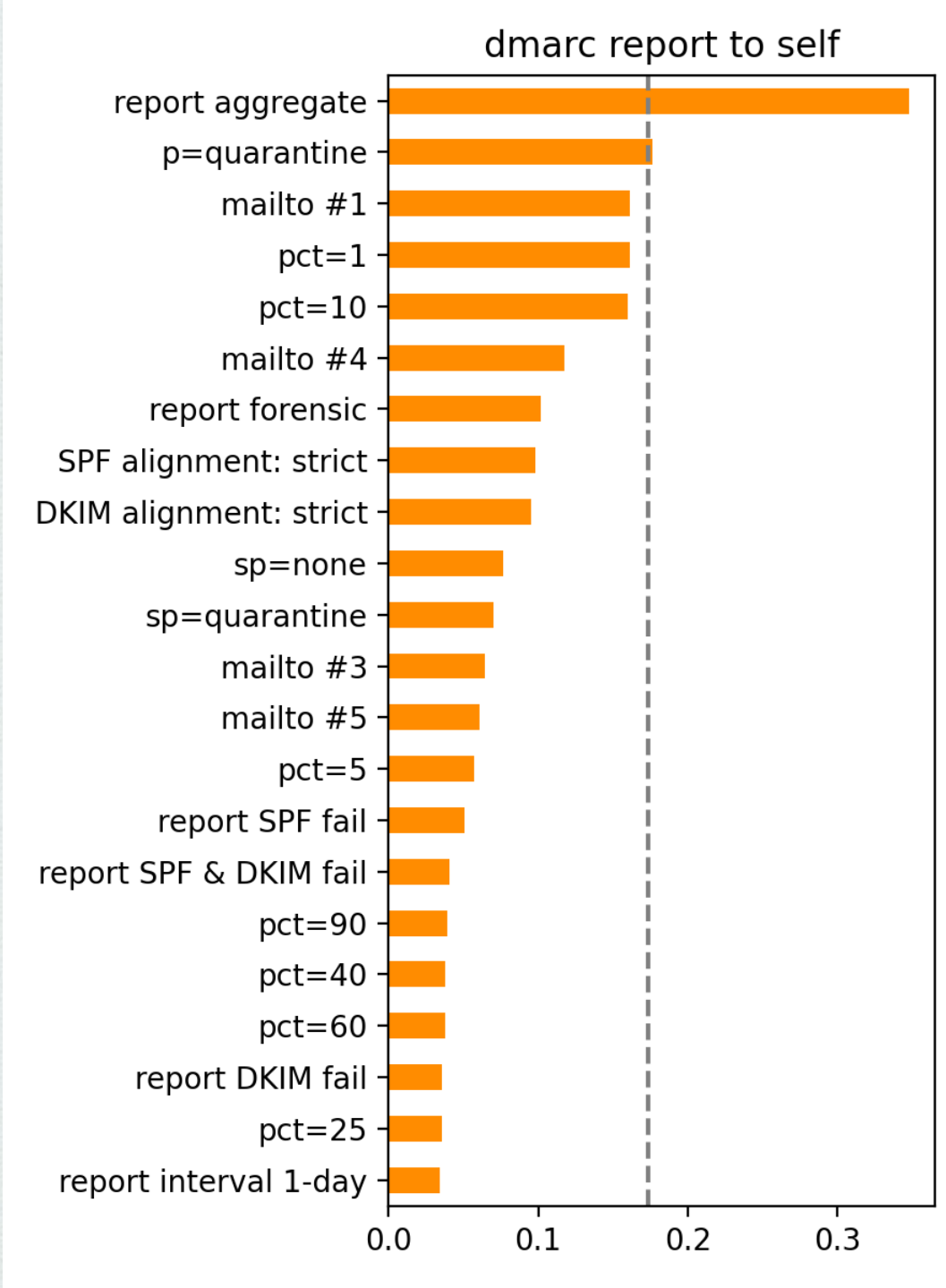
DMARC Provider	RUA/RUF Server	Percentage
Non-EU Company	Outside EU	
EU Company	Outside EU	33%
Non-EU Company	Inside EU	
EU Company	Inside EU	
Self	Self	35%

Send Reports to Self

Instruct receivers when to generate & send aggregate & message-specific info

Notable details:

- Policy for self: Quarantine
- Policy for subdomains: None, Quarantine
- Report criteria: When SPF fail, both SPF & DKIM fail, DKIM fail
- SPF & DKIM alignments: ‘strict’ (‘strict’ = exact FQDN match & ’relaxed’ = otherwise)
- Report interval: 1 day
- Emails to apply policy on: 1%, 10%, 5%
- Report type: aggregate, forensic



Key Points

DMARC Policy Caching

DMARC records with a long DNS TTL (Time-To-Live) can cause a critical change to parameters to go unnoticed for the length of the TTL

DMARC Policy Options

Email domain owner can inform the Mail Receivers how they should treat emails that pass/fail the DKIM/SPF checks: do nothing, quarantine or reject

DMARC Reports

Aggregate Reports (RUA) give an overview of email authentication results.

Forensic Reports (RUF) provide detailed information about individual failed emails

SPF/DKIM Alignment

Email domain owner would use strict-mode for emails with exact DNS domain match, and relaxed-mode to include subdomains

PCI Security Standards Council®

2025 EUROPE COMMUNITY MEETING