From Matrix to Metrics: Introducing and Applying a Configuration Matrix to Evaluate DMARC Policies

Tobias Länge*, Fabian Lucas Ballreich*, Anne Hennig*, Peter Mayer* and Melanie Volkamer *
* Karlsruhe Institute of Technology (KIT), Karlsruhe, Germany
{tobias.laenge, fabian.ballreich, anne.hennig, peter.mayer, melanie.volkamer}@kit.edu

***Abstract*—Email spoofing, the practice of sending illegitimate messages that appear to come from a legitimate sender, is a phishing technique frequently employed by attackers. In an effort to prevent such phishing, anti-spoofing mechanisms like DMARC were introduced and have been examined in the research community with respect to describing adoption rates, policies used, and potential problems. However, prior research has not yet taken into account all aspects of DMARC when evaluating how effectively configurations prevent spoofing attacks. To address this research gap, we developed a utility-oriented configuration matrix – focusing on the anti-spoofing effectiveness of different DMARC configurations – and provide clear recommendations for selecting the appropriate configuration. We then collected data from the Tranco Top-100k list daily for a duration of eight months and applied our classification to the collected data. Our analyses of the collected data reveals how configurations evolve over time and provides insights into the actual deployment of DMARC in practice. This allows us to identify potential issues that hinder the adoption of more secure configurations and to identify the most common errors in invalid DMARC records found in the wild, which could serve as a basis for enhancing the DMARC standard. Our results show that domains move towards configurations that are more effective against email spoofing, however, still exhibiting a lack of knowledge with respect to different policy settings.**

I. Introduction

Email continues to be a highly utilized medium for communication, even as newer collaboration tools such as instant messaging and video conferencing become more prevalent. It remains especially common within corporate, governmental, and organizational contexts because it is inexpensive, straightforward to implement, and requires minimal user training. The foundational email architecture [1], developed in the 1980s, was designed with limited built-in security, a weakness that attackers exploit, for instance, through phishing attacks.

Attackers utilize phishing messages to learn sensitive information such as login credentials, personal or organizational information, or to install malware [2]. Phishing attacks constitute a substantial proportion of all cybersecurity incidents.

A major reason for that is the trust that recipients place in the sender's claimed identity. If a recipient trusts the stated sender, they are more inclined to disclose sensitive information or comply with the message's request, thereby strengthening the impact of malicious communications [3]. At the same time, email spoofing is a frequently used phishing technique in which the sender information of an email is forged, allowing the attacker to gain the recipient's trust [4].

In response to these conceptual vulnerabilities of email communication and the underlying Simple Mail Transfer Protocol (SMTP), the email system has progressively incorporated additional security mechanisms to mitigate the weakness of the original protocol, such as Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-Based Message Authentication, Reporting, and Conformance (DMARC). Among these, DMARC has emerged as an authentication protocol for preventing email spoofing. DMARC allows domain owners to publish a policy that instructs receiving email servers on how to handle messages that fail specified authentication checks and directs the reporting of aggregate data back to the sending domain. DMARC adoption has increased in recent years [5], partially driven by companies like Yahoo, Google, and Microsoft [6] requiring it. But setting up DMARC is only the first step, configuring it correctly is another challenge in itself. Kondo et al. [7] found that in 2025 less than 20% of domains use an effective DMARC implementation. Unfortunately, the authors did not clarify what constitutes an "effective" implementation, which can lead to misunderstandings and less effective configurations.

With our work we aim to contribute to a better understanding of DMARC adoption, and provide best practices for correctly implementing DMARC to achieve effective protection against email spoofing. We address this by (1) proposing a configuration matrix of different sets of DMARC configurations based on their protection against spoofing attacks and reporting effectiveness (Section IV). Based on this configuration matrix, we (2) conducted an eight-month measurement study analyzing the DMARC configurations of the Tranco top 100k most popular domains (Section V). This allows us to gain insight into the practical application of DMARC and to evaluate associated weaknesses and opportunities for improvement. Furthermore, by performing daily scans, we are able to describe changes and transitions in configurations for each of the domains in our sample. This helps to identify the implementation approaches used in practice, and if configurations are adjusted after initial setup. Moreover, (3) we identify the most common errors present in invalid DMARC records of these domains and categorize them (Section VI-E).

Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb) 2026
27 February 2026, San Diego, CA, USA
ISBN 978-1-970672-06-0
https://dx.doi.org/10.14722/madweb.2026.23031
www.ndss-symposium.org

II. Technical Background

To transfer an email from one server to another, the Simple Mail Transfer Protocol (SMTP) is used. In the context of email security, it is important to differentiate between the *envelope-From* and *message-From*. The first is part of SMTP and mainly used during the communication between the two email servers. The *message-From* on the other hand is the actual email header shown to the user in most email clients.

This allows for email spoofing where an attacker falsifies the *message-From* address in an email so it appears to come from a trustworthy sender. There are legitimate use cases, such as email forwarding, but also malicious ones, such as spam and phishing. To tackle email sender spoofing, SPF, DKIM, and DMARC were introduced as optional security measures.

A. Sender Policy Framework (SPF)

The Sender Policy Framework (SPF) was introduced in its current form in RFC 7208 [8] and RFC 7372 [9], giving the receiving email server a method to verify if the sending mail server is authorized to send emails from a specific domain. To do so, the owner of a domain publishes a DNS record with a list of IP addresses of all email servers that are authorized to send emails on their behalf. The receiving email server can now look up the SPF entry for the domain specified in the *envelope-From* field and compare it to the IP address of the server trying to transmit the email. It is important to note that this only verifies the *envelope-From* domain, not the sender specified in the *message-From* header.

B. DomainKeys Identified Mail (DKIM)

DomainKeys Identified Mail (DKIM) is defined in RFC 6376 [10] and mitigates email spoofing by adding a header with a digital signature to outgoing emails. This allows the receiving party to verify that the body and some headers, including the *message-From* header, were not modified. One issue with DKIM is that if a server receives an email without a DKIM signature, it remains unclear whether the sender does not use DKIM or the message was sent by a malicious actor.

C. Domain-based Message Authentication, Reporting and Conformance (DMARC)

Domain-based Message Authentication, Reporting and Conformance (DMARC) is defined in RFC 7489 [11] and gives the owner of a domain the option to specify a policy how to verify the authenticity of emails sent on their behalf. For this, DMARC specifies how the receiving email server should handle failed SPF or DKIM checks. Additionally, DMARC also verifies the alignment of the *message-From* domain with the domains used for the SPF and DKIM checks. The second feature of DMARC is the option to set up reporting for failed authentication checks, offering the domain owner additional information about potential misuse of their domain. A DMARC entry is published as a DNS record on the subdomain *_dmarc*, e.g., *_dmarc.example.com* for the domain *example.com*. Several tags must or can be specified:

- **v (required)** – version tag: Currently always *DMARC1*
- **p (required)** – policy tag: Must be *none*, *quarantine* or *reject*. This defines how the recipient should proceed with emails that fail the DMARC check.
- **sp (optional)** – sub-domain policy tag: Default value is the same as **p**. Applied to all subdomains that do not have their own DMARC record.
- **pct (optional)** – percentage tag: Percentage (0–100) of messages to which the policy is applied: default value is 100.
- **rua (optional)** – URI(s) for aggregate reports (e.g. `mailto:dmarc@example.com`).
- **ruf (optional)** – URI(s) for forensic reports.
- **fo (optional)** – failure-report options:
  - `0` – generate report only if both SPF *and* DKIM fail (default).
  - `1` – generate if either SPF *or* DKIM fails.
  - `d` – generate if DKIM fails.
  - `s` – generate if SPF fails.
- **adkim (optional)** – DKIM alignment mode: *r* (relaxed) or *s* (strict).
- **aspf (optional)** – SPF alignment mode: *r* (relaxed) or *s* (strict).
- **ri (optional)** – report interval in seconds; default value is 86400 (24 h).
- **rf (optional)** – report format for forensic reports; default value is *afrf*.

In October 2023, Google and Yahoo announced that they require senders who send 5,000 or more emails per day to either provider to implement DMARC starting in February (Yahoo) and June (Google) 2024. Microsoft joined this initiative in May 2025. Current requirements include implementing SPF, DKIM, and publishing a valid DMARC record with at least the policy p = *none*. Microsoft explicitly recommends using the *reject* policy, while Yahoo and Google state that p = *none* is sufficient in the beginning. All three recommend using reporting, but do not require it. If the requirement is not enforced, all providers state that emails may be forwarded to SPAM or be rejected [12], [13], [14].

III. Related Work

Soon after the first specification of DMARC was published, several researchers began to measure DMARC adoption rates (e.g., [5], [15], [16], [17], [18], [19]). While measurements show adoption rates below 5% before 2019 (e.g., [20], [15], [21]), DMARC adoption continuously increased (e.g., [5], [20]). Latest measurements exhibit an adoption rate of approximately 50% [7] among the top domains in the Tranco 1 Million list. Related work has also found that, especially on the subdomain level, adoption is low [17], while adoption is higher for higher-ranked domains [22], [16]. When specifically analyzing reporting functions, Ashiq et al. [18] found that only around 35% – 55% of the domains that use DMARC also activated reporting functions.

DMARC is described as most effective when strict policies are enforced by domain owners [23], [24], and it is pointed

out that the lack of SPF and DMARC carries the risk of domains being used to send spoofed emails [17], [24]. Maroofi et al. [25] identified further attack scenarios, such as subdomain spoofing. Additionally, Ashiq et al. [18] demonstrated that misconfigurations in reporting functions (e.g., missing DMARC authorization records when reporting is directed to an external domain) can lead to Denial-of-Service by using reflection attacks.

Recommendations on "effective" DMARC implementations in related work range from providing best practices for implementations to rather organizational recommendations, such as streamlining configurations [26] or improving the RFC [25]. Dakic et al. [26] describe a step-wise DMARC implementation process that should have p = *reject* as a goal. However, the authors did not provide recommendations on reporting mechanisms, which Ashiq et al. [18] identified as a potential source of misconfiguration. Zhang et al. [17] also provide rather generic recommendations, such as setting p and sp tags to reject or quarantine, enabling rua and ruf functions, and periodically reviewing the reports without explaining how these settings increase e-mail security. Hureau et al. [27] provided a more extensive description that included all tags individually. However, the authors did not provide a comprehensive classification combining all the tags.

As a result of the less tangible recommendations, especially less strict configurations are common, indicating that domain owners lack a proper understanding of which configuration provides the most protection against spoofing attacks. In 2021, Tatang et al. [16] found that almost 75% of DMARC entries use p = *none*, the least strict configuration. This has not, on average, increased over time, as Kondo et al. [7] measured in 2025 a general DMARC adoption rate for the Tranco 1 Million list of around 50%, but only less than 20% use an "effective" implementation (i.e., p = *reject* or p = *quarantine*). From a provider's perspective, Blechschmidt et al. [19] also found that although most of the email providers they investigated in their study specify DMARC at a relatively high rate (37/47), they often do not enforce DMARC [19].

In an effort to define the most effective implementation to distribute to email server administrators, we sought to identify the difference between "effective" and "non-effective" implementations, including optional tags such as pct and sp. While Dakic et al. [26] highlighted "effective" implementation as crucial, no paper has yet provided a comprehensive classification that can be used to a) address misconceptions about "correct" implementations which were identified by Blechschmidt et al. [19], b) address lack of knowledge as identified by Zhang et al. [17], c) address misunderstandings and difficulties as raised in Hu et al. [15]. Therefore, the main goal of our study was to develop a configuration matrix to classify DMARC configurations based on their protection against spoofing attacks and reporting effectiveness.

IV. Proposed DMARC Configuration

As described in Section II-C there are many different parameters that can be configured for DMARC. Previous work mainly focused on single aspects, e.g., the adoption rate of DMARC [5], the selected policy [5], selected subdomain policy [5], or a combination of policy and reporting options [27]. However, looking at single aspects of the DMARC configuration does not provide the complete picture. To better understand the effectiveness of real world DMARC configurations against email spoofing, we need to consider all of them. Because different configurations yield similar results, we classified DMARC configurations by their potential to protect against spoofing attacks and their ability to produce informative reports for domain owners.

First, we examine the DMARC parameters specified in the RFC that are relevant to effective spoofing protection. Based on this, we present our proposed classification for DMARC configurations. We perform our classification based on the DMARC implementation according to RFC 7489 [11] and expect it to be correctly implemented by the receiving email server. Also, we do not consider other countermeasures against email spoofing, e.g., spam filters, as they are not standardized and therefore unpredictable.

A. Relevant DMARC parameters

To identify how the configuration of the different parameters influences the protection against spoofing attacks, we assume that we are responsible for the domain *example.com* – that is, that we are the domain owner. The attacker's goal is to send a spoofed email with the *message-From* header set to an address associated with our domain *example.com*, e.g., *support@example.com*. If we do not set a DMARC record for our domain, an attacker can send an email in our name. They do not face any issues, and the email is sent without us noticing the attack.

When we configure a DMARC record, the receiving mail server receives instructions on what actions should be taken for emails that are illegitimately sent in our name. This gives us the option to instruct the receiving email server on (1) how to handle illegitimate emails and (2) sending a report about it back to us. The relevant tags to instruct the receiving email server about these actions are the policy tag, the subdomain policy tag, the percentage tag, and the URI(s) for reports.

a) Policy Tag (p): The policy tag can be set to *none*, *quarantine*, or *reject* and is required. If it is set to *none*, the attacker can still use *support@example.com* without issues, as it instructs the receiving email server to take no action. If set to *quarantine*, the receiving email server is instructed to label the email as spam or similar. This makes it more difficult for an attacker to convince a potential recipient, as the recipient might not even see the email. Setting the policy tag to *reject* instructs the receiving email server to reject the email before it's delivered to the recipient. As, in this case, the recipient will never see the illegitimate message, setting the policy tag to *reject* will successfully prevent such a phishing attack.

b) Subdomain Policy Tag (sp): If the subdomain policy tag is set to a weaker policy than the policy tag (e.g., p = *reject* and sp = *none)*, it allows an attacker to use a fictitious subdomain of our legitimate domain as sender,

e.g. *john.doe@support.example.com*. This attack scenario was described by Maroofi et al. [25]. Therefore it is important to set the sp tag to at least the same policy as the p tag. Otherwise the effectiveness of the p tag is reduced.

c) Percentage Tag (pct): The policy tag will only enforce the respective action if the percentage tag is set to 100%, the default value. If it is set to any lower percentage, the policy is no longer enforced on all emails, but only on the respective percentage of emails. For all emails where the policy is not enforced due to the pct tag, the next lower restrictive policy is applied. If, for example, the policy tag is set to *quarantine* and $pct = 50$, every second mail will be treated as if the policy is set to *none*. Due to the inconsistent enforcement, this is not advised, because an attacker could simply circumvent the stricter policy by sending more emails.

d) Report URI(s) (rua, ruf): There are two reporting options defined for DMARC, rua and ruf. These specify the Uniform Resource Identifier(s) (URI) where the receiving email server should send reports to. The two options differ in the format of the report, but both inform us about possible spoofing attacks using our domain. Setting up the report URI(s) does not prevent the attacker from successfully delivering the email to a recipient, but gives us, the domain owner, the option to act. If we learn from the reports that a phishing campaign is using our domain, we can, e.g., send emails to our customers informing them about the attack. Although this has only a limited effect on phishing prevention, we believe it still offers an essential benefit for detecting and combating phishing campaigns at an early stage. We do not differentiate between setting up rua or ruf. Practice has shown that rua is more effective as some receiving email servers might not send ruf reports due to privacy concerns. [28] Therefore rua is recommended.

e) Other Tags: The remaining DMARC tags have little to no influence on the protection of the recipient. The fo, ri, and rf tags can be used to adjust details of the reporting mechanism. But in any case, reports are sent to the defined URI(s) on DMARC check failures. The adkim and aspf options might be useful for organizations that need strict separation between subdomains.

B. DMARC configurations

With these insights in mind, we categorize the different parameters for these tags based on their benefit for (a) the recipient and (b) the domain owner of the spoofed domain.

a) Protection for the recipient: Regarding configurations that protect the recipient, we defined four categories based on how effective they are at protecting the recipient. (1) The first category covers configurations where the effective policy is *none* for all emails. That is the case if one of the policies, p or sp, is set to none. Or if one of the policies is set to *quarantine* and the percentage, pct, is set to 0%. Because in this case the next lower restrictive policy, *none*, will be applied. For these configurations, the receiving email server is instructed to take no further action, i.e., neither to block nor to label any received emails. Therefore, this category does not protect the recipient from email spoofing. (2) The second category covers configurations where a stricter policy, *quarantine* or *reject*, is not enforced consistently. Some incoming emails will be treated as if the policy is set to *none* by the receiving email server. This is the case if one of the policies is set to *quarantine* and the other to *quarantine* or *reject*, and the percentage is between $1\% - 99\%$. Therefore, this category provides only slightly better protection from email spoofing for the recipient, as some, but not all potential phishing emails with spoofed senders are delivered. (3) This category covers all configurations where both policies are set to a minimum of quarantine, but not both to reject. So, for this category, all emails will be at least labeled as spam by the receiving email server. This provides the recipient with an indicator that the email is illegitimate. (4) The last category covers all configurations that enforce *reject* consistently. This occurs when both policies are set to *reject* and the percentage is 100%. The receiving email server will reject messages with spoofed senders, preventing phishing emails from reaching the recipient's inbox. This setting provides the best protection for the recipient.

b) Reports for the domain owner: For the domain owner, we defined two categories of configurations. (A) If both ruf and rua are not defined, the domain owner is not informed about failed DMARC checks by the receiving email servers. Therefore, the domain owner will not be informed about emails sent on their behalf and cannot react to them. (B) If at least one of the tags ruf or rua is set to a valid URI, the domain owner is notified about failed DMARC checks by the receiving email servers. As described above, the reports allow the domain owner to respond to the spoofing attack promptly and, based on the reports, inform their users or take other appropriate actions.

Based on these two groups, the perspective of the recipient and the domain owner, we created the configuration matrix with eight different categories, as shown in Table I.

c) Recommendations: Based on our categorization, we can see that configuration 4B (see Table I) provides the greatest benefit to both the recipient and the domain owner. It prevents spoofed emails from being delivered to the recipient and provides the domain owner with reports about failed DMARC checks. Therefore, we recommend 4B as the target configuration. It should be the goal to reach this configuration.

During initial setup of DMARC, misconfigured SPF or DKIM configurations can cause false positives. That is why we recommend to initially set the DMARC configuration to 1B – specifying a DMARC record and enabling reporting – before later changing it to 4B. This provides the domain owner with the information needed to detect potential issues without risking legitimate emails being rejected.

As for the other categories, we do not recommend category A configurations, as they provide no insights about failed DMARC checks to the domain owner. Neither during initial rollout to detect false positives, nor later to detect illegitimate emails being sent. For the remaining configurations, 2B and 3B, there is no advantage over 1B during the initial setup.

TABLE I
DMARC CONFIGURATION MATRIX

		Reports for Domain Owner	
		[A] rua AND ruf not set	**[B] rua OR ruf set**
Protection for Recipient	**[1]** $(\mathbf{p} = \mathbf{none} \ \vee \ \mathbf{sp} = \mathbf{none}) \vee (\mathbf{pct} = 0 \ \wedge \ \mathbf{p} \neq \mathbf{reject} \ \wedge \ \mathbf{sp} \neq \mathbf{reject})$	**[1A] No benefit for recipient; No reports for Domain Owner**	**[1B] No benefit for recipient; Reports for Domain Owner**
	[2] $(\mathbf{p}, \mathbf{sp}) \in \{\mathbf{reject}, \mathbf{quarantine}\}^2 \setminus \{(\mathbf{reject}, \mathbf{reject})\} \wedge 1 \leq \mathbf{pct} \leq 99$	**[2A] Inconsistent benefit for recipient; No reports for Domain Owner**	**[2B] Inconsistent benefit for recipient; Reports for Domain Owner**
	[3] $\big[(\mathbf{p}, \mathbf{sp}) \in \{\mathbf{reject}, \mathbf{quarantine}\}^2 \setminus \{(\mathbf{reject}, \mathbf{reject})\} \wedge \mathbf{pct} = 100\big] \vee \big[p = \mathbf{reject} \wedge sp = \mathbf{reject} \wedge \mathbf{pct} < 100\big]$	**[3A] Illegitimate emails marked as spam for recipient; No reports for Domain Owner**	**[3B] Illegitimate emails marked as spam for recipient; Reports for Domain Owner**
	[4] $(\mathbf{p} = \mathbf{reject} \ \wedge \ \mathbf{sp} = \mathbf{reject}) \wedge \mathbf{pct} = 100$	**[4A] Illegitimate emails rejected; Greatest benefit for recipient; No reports for Domain Owner**	**[4B] Illegitimate emails rejected; Greatest benefit for recipient; Reports for Domain Owner**

In fact, they only increase the risk of legitimate emails being rejected due to misconfiguration. While 3B provides higher protection for the recipient compared to 1B, it should not be considered a preferred configuration, as it still offers less protection than 4B and does not provide any other benefits.

C. Summary

We categorized the possible combinations of DMARC parameters into eight distinct configurations (1A – 4B). Based on the effectiveness in preventing email spoofing and notifying the domain owner about abuse, we recommend the following configurations: During the initial setup of DMARC for a domain, we recommend configuration 1B. After any potential issues have been resolved, the configuration should be set to 4B to enable the greatest DMARC protection mechanisms.

V. Data Collection

As described in Section I, we next conducted an eight-month measurement of the DMARC adoption to gain insights into which DMARC configurations are present in the wild.

A. Sample

As a basis for our data collection, we used the Tranco list, available at https://tranco-list.eu/list/KJYZW [29], generated on Feb. 10, 2025. This list contains only pay-level domains, as we want to analyze DMARC usage for domains that are likely to be spoofed and where we can see the effect of the *sp* tag. Therefore, it excludes subdomains and technical domains, like APIs or CDNs, that most users would not even recognize as a trustworthy domain. We used the first 100k domains from the aggregated and filtered list as our sample, which we scanned on a daily basis between 04/2025 and 12/2025.

B. Retrieving DMARC entries

To collect data on the current state of DMARC adoption in our sample, we implemented a scanner in Python using the *checkdmarc*[1] library. Our scanner collects all relevant data, mainly the DMARC records, that we used to categorize the domains based on our proposed configuration matrix. *Checkdmarc* collects the DMARC record and parses it during data collection, making it easier to analyze the data later.

C. Handling of DNS errors

To prevent issues arising from special DNS rules on our institutional DNS server, we used the public DNS server of Cloudflare, 1.1.1.1. To further reduce the likelihood that connection issues affect our data, we ran the *check_domains* function up to 3 times if no result was obtained. We canceled the check for this domain after the third attempt failed to produce a result. As timeout for the *check_domains* function, we used the default value of 2 seconds.

D. Data pre-processing

Our data collection script provides all the necessary data to categorize the domains according to our proposed configuration matrix. To do so, we processed the data for each day in the following steps:

1) Find missing domains: We compare the retrieved data set with the list of domains that were checked. All domains missing from the data set are marked as no_data for that day.
2) Mark invalid results: We check the data for DNS errors. That is, if we do not receive a result from the nameserver or if the domain does not exist (NXDOMAIN). These domains are marked as $invalid\_data$ for that day.
3) Mark domains without DMARC: From the valid data, we filter out all domains that have no DMARC record. These domains are marked as no_dmarc for that day.
4) Mark invalid DMARC records: From the data with a DMARC record, we filter out all domains that failed the parsing of the DMARC record by *checkdmarc*. These domains are marked as $dmarc\_invalid$ for that day.

[1]https://github.com/domainaware/checkdmarc, version 5.3.1

5) Categorize DMARC records: The valid DMARC records are then categorized based on our configuration matrix. We filter the domains based on their effective values for p, sp, pct, rua and ruf to assign them to their corresponding category 1A – 4B for that day.

VI. Data Analysis

In the following, we describe the results of our measurement study. First, we describe the initial state of the examined sample of the Tranco top 100k list with respect to the existence of DMARC records and their distribution across the various possible configurations defined in Section IV. We then trace the development over the entire timeframe, highlighting noteworthy trends and changes. Next, we look at the transitions between configurations for each domain, first comparing the initial with the final state and then on a daily basis. This gives us insight into how configurations change over time. Finally, we examine the subset of DMARC entries that contain syntactic or semantic errors and therefore do not conform to the RFC. These entries are grouped into categories to better understand the types of problems domain owners encounter when applying DMARC.

A. Initial situation

First, the initial state at the time of the first data scan (2025-04-01) was examined. In the sample of 100k scanned domains, we could not retrieve data for 2.0% (2029) of the domains due to DNS errors (2016) or other errors (13). 42.4% of the scanned domains did not publish a DMARC record. This makes a total of 44.4% of the scanned domains that would not be subject to a DMARC policy, and therefore, from now on, are treated as having no DMARC record. That leaves 55586 (55.6%) domains with a DMARC record that can be retrieved via a DNS query. Of these DMARC records, 1.1% (which corresponds to 0.6% of the entire sample) contain syntactic or semantic errors that violate the RFC specification. The remaining 98.9% of the existing records are free of such errors and are therefore classified by us as *valid*. Hence, 55.0% of all domains in the sample possess a valid DMARC record.

Focusing on the configurations defined in Section IV, 21.8% of the valid DMARC records (12.0% of the entire sample) fall into category A with no reporting address specified. Receiving email servers are therefore unable to send reports about failed DMARC checks to the domain owner, leaving the owner without an overview of attempted spoofing attacks or technical problems. Within this category, configuration 1A has the largest share, accounting for 15.5% of all valid records. This configuration offers no security advantage, as failed tests on the recipient side do not affect the handling of the email (see Section IV). Configuration 2A is present in our sample only at 0.1%. The more secure configurations, 3A and 4A, account for 3.3% and 2.9% of all valid DMARC records, respectively. This means that a total of 6.2% of domains with a DMARC record have an entry that, while not defining a reporting address, at least defines a policy that specifies *quarantine*.

TABLE II
Distribution of configurations 1A - 4B for 2025-04-01 in relation to all valid DMARC entries

		Reports for Domain Owner	
		[A] rua AND ruf not set 11.987 domains (21.8%)	**[B] rua OR ruf set 42.974 domains (78.2%)**
Protection for Recipient	**[1]** $(\mathbf{p} = \mathbf{none} \ \vee \ \mathbf{sp} = \mathbf{none}) \vee (\mathbf{pct} = 0 \ \wedge \ \mathbf{p} \neq \mathbf{reject} \ \wedge \ \mathbf{sp} \neq \mathbf{reject})$ **28.133 domains (51.2%)**	**[1A] 8.508 domains (15.5%)**	**[1B] 19.625 domains (35.7%)**
	[2] $(\mathbf{p}, \mathbf{sp}) \in \{\mathbf{reject}, \mathbf{quarantine}\}^2 \setminus \{(\mathbf{reject}, \mathbf{reject})\} \wedge 1 \leq \mathbf{pct} \leq 99$ **983 domains (1.8%)**	**[2A] 75 domains (0.1%)**	**[2B] 908 domains (1.7%)**
	[3] $[(\mathbf{p}, \mathbf{sp}) \in \{\mathbf{reject}, \mathbf{quarantine}\}^2 \setminus \{(\mathbf{reject}, \mathbf{reject})\} \wedge \mathbf{pct} = 100] \vee [p = \mathbf{reject} \wedge sp = \mathbf{reject} \wedge \mathbf{pct} < 100]$ **11.163 domains (20.3%)**	**[3A] 1.810 domains (3.3%)**	**[3B] 9.353 domains (17.0%)**
	[4] $(\mathbf{p} = \mathbf{reject} \ \wedge \ \mathbf{sp} = \mathbf{reject}) \wedge \mathbf{pct} = 100$ **14.682 (26.7%)**	**[4A] 1.594 domains (2.9%)**	**[4B] 13.088 domains (23.8%)**

The remaining 78.2% of the valid DMARC records (43.0% of the total sample) belong to category B, all of which define at least one reporting address within their DMARC record. Analyzing DMARC reports provides clear insights into legitimate and illegitimate email sendings, enabling targeted countermeasures against spoofing attempts (i.e., warning customers). Furthermore, reports allow for the detection of incorrect SPF/DKIM settings, e.g., if third-party contractors are used for sending out emails.

Within category B, configuration 1B holds the largest share, accounting for 35.7% of all valid DMARC records. This means that the domains have configured at least one reporting address, yet their DMARC policies are such that failures detected on the recipient side do not influence how the messages are handled. This is the configuration we recommend when initially deploying DMARC for a domain. Configuration 2B, which, unlike 1B, enforces *quarantine* or *reject* inconsistently, accounts for only 1.7% of the valid DMARC entries. In contrast, configuration 3B, which enforces at least *quarantine* for all emails, accounts for 17.0% of all DMARC entries.

Configuration 4B, defined as our target configuration (see Section IV), specifies at least one reporting address and requires "reject" for all emails. 23.8% of the valid DMARC records match this target configuration. Across all 100k examined domains, this corresponds to 13.1% of the sample. The results are shown in Table II.

B. Development of DMARC adoption over time

After examining the initial state, we looked at how the values changed over the data collection period. For the sake of simplicity, for each month, we used the scan conducted on the first day of the month as a single data point, producing a total of nine observations ranging from 01 April 2025 to 01 December 2025.

Figure 1 illustrates the increase in the proportion of valid DMARC records for the entire sample over the study period. The adoption rate of DMARC, which started at 55.6%, rose by 2.8 percentage points to reach 58.4%.

Figure 2 compares the development of domains that lack a DMARC record with the share of domains that possess the

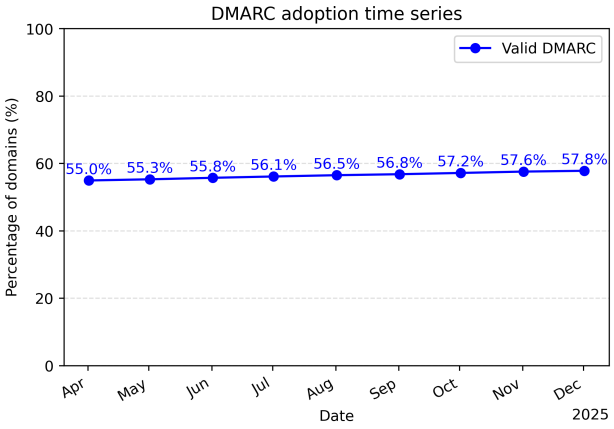

Fig. 1. Increase in number of domains with a valid DMARC record over the observation period.

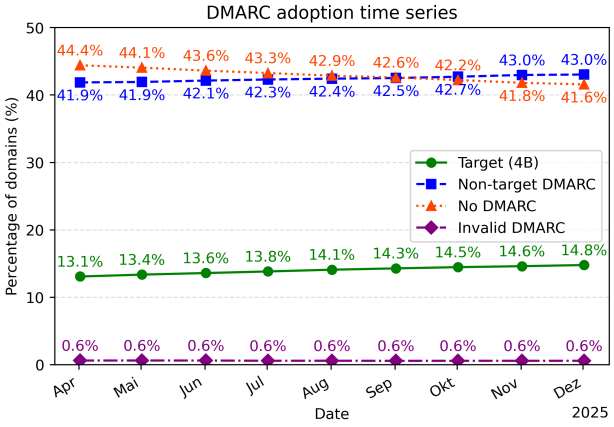

Fig. 2. Comparison of the percentage of domains without a DMARC record (orange) with domains with a valid DMARC record according to the target configuration 4B (green), domains with a valid DMARC record according to other non-target configurations (blue) and domains with an invalid DMARC record (purple).

target configuration 4B, those with a non-target configuration, and those with an invalid DMARC record. As mentioned before, other errors, – mainly DNS related – were counted towards "no DMARC". The proportion of invalid DMARC records remained constant at roughly 0.6% of all domains throughout the observation period. The share of domains without any DMARC record fell from 44.4% to 41.6% (a decrease of 2.8 percentage points), whereas the share of domains with the target configuration increased from 13.1% to 14.8% (1.7 percentage points). At the same time, the proportion of domains with a non-target configuration also increased from 41.9% to 43.0% (1.1 percentage points).

C. Category Transitions between Initial and Last Scan

The development described above raises the question of whether the domain owner directly transitions from "no DMARC" to the target configuration, or proceeds through an intermediate non-target configuration. To investigate this, we

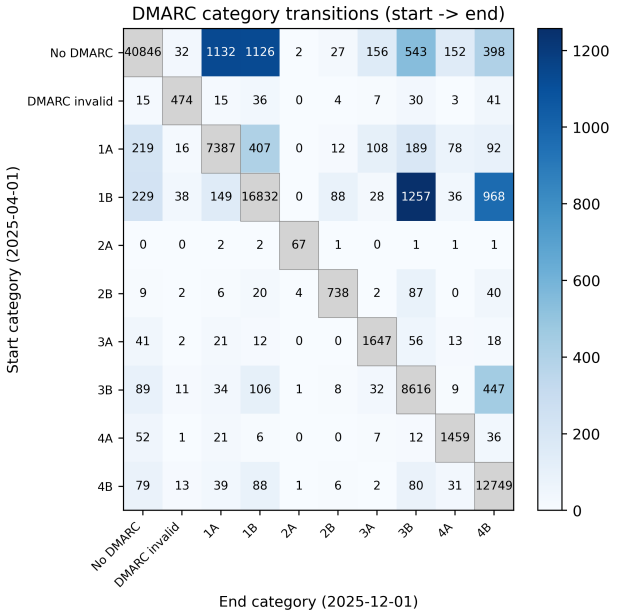

Fig. 3. The figure shows the absolute count of domains that moved from the configuration indicated on the left to the configuration displayed on the bottom during the observation period. The sum of all values in a row corresponds to the absolute value of the respective category at the first data point 2025-04-01, the sum of all values in a column corresponds to the absolute value at the last data point 2025-12-01. "No DMARC" includes domains that were no longer reachable – *invalid_data* and *no_data* (see Section V-D)

conducted a per-domain analysis of changes in the individual configurations over the eight months. Figure 3 visualizes the transitions between the different DMARC configurations observed during the measurement period. The configurations comprise domains that lack a DMARC record, domains with an invalid DMARC record, and the various valid configurations defined by our configuration matrix in Section IV.

When examining the transitions that originate from the "No DMARC" state, the largest movements are to configuration 1A (1132 domains) and configuration 1B (1126 domains). After these, the next most frequent transition is to configuration 3B (543 domains), followed by a movement to our target configuration 4B (398 domains). This indicates that configurations 1A and 1B are the most common entry points into a valid DMARC implementation.

Focusing on the target configuration 4B, the majority of transitions (968 domains) arrive there from configuration 1B. This observation supports our recommendation of configuration 1B as an appropriate starting point. The next-largest source for 4B is configuration 3B (447 domains), followed by "No DMARC" (398 domains). A similar pattern is noticeable for transitions into configuration 3B. The most frequent source is configuration 1B, with 1257 domains moving to 3B, whereas transitions from the "No DMARC" state represent 543 domains, a substantially lower number. To summarize, these results suggest that in practice, many domains follow the transitions "No DMARC $\rightarrow$ 1B $\rightarrow$ 3B $\rightarrow$ 4B". Additionally, a considerable number of domains move directly between "No

TABLE III
DISTRIBUTION OF THE FREQUENCY OF TRANSITIONS BETWEEN DMARC CONFIGURATIONS DURING THE COLLECTION PERIOD.

number of transitions	count	%
0	89316	89.33%
1	7477	7.48%
2	2415	2.42%
3	512	0.51%
4	139	0.14%
5	56	0.06%
6	22	0.02%
7	11	0.01%
$\geq$8	52	0.05%
Total	100000	100%

DMARC" and configuration 1A. From 1A, the largest proportion of domains transition to 1B (407 domains), implying that in practice, 1A is also frequently used as an intermediate configuration before adopting 1B, thereby finally enabling the target configuration 4B.

Interestingly, Figure 3 also shows some domains that regress in configuration, e.g., from the target configuration 4B to 1B or even from 4B to "No DMARC".

D. Transitions on a daily basis

To obtain a more fine-grained view on the dynamics between different DMARC configurations, we performed an analysis of every transition that occurred during the observation period, not only the configurations at the start and end. Leveraging the daily scans of all monitored domains, we tracked not only individual configuration changes but also the sequences of successive changes that a domain experienced.

Table III presents the distribution of the frequencies of the number of transitions during the observed period. Across the entire sample, 89.33% of the domains retained the same configuration throughout the observation period, whereas 10.67% of the domains underwent at least one configuration change during the study period. The vast majority of these (9.89%) underwent one (7.48%) or two (2.42%) transitions within the period; only a small part (0.78%) had more.

Therefore, focusing on transition sequences originating from "No DMARC" at the start of the observation period towards a valid DMARC configuration – shown in Table IV – draw a similar picture as the results in Section VI-C. This confirms that most domains start out with configuration 1A or 1B, followed by 3B and 4B.

We performed the same analysis for transition sequences ending in the target configuration 4B, shown in Table V. Most transitions are from a different DMARC category to 4B, with only 18.6% directly coming from no DMARC configuration, confirming our results in Section VI-C

For the subset of domains that changed, Table VI lists the most frequently observed configuration sequences. The percentages reported in the table correspond to the share of all domains that changed at least once.

TABLE IV
DISTRIBUTION OF THE FIRST TRANSITIONS ORIGINATING FROM "NO DMARC" AT THE START OF THE OBSERVATION PERIOD TOWARDS A DMARC CATEGORY. NOTE: THESE VALUES ALSO INCLUDE DOMAINS THAT UNDERWENT FURTHER TRANSITIONS AFTER THIS INITIAL CHANGE.

Entry configuration	Count	%
No DMARC $\rightarrow$ 1A	1278	31.4%
No DMARC $\rightarrow$ 1B	1281	31.5%
No DMARC $\rightarrow$ 3B	662	16.3%
No DMARC $\rightarrow$ 4B	499	12.3%
No DMARC $\rightarrow$ 4A	188	4.6%
No DMARC $\rightarrow$ 3A	139	3.4%
No DMARC $\rightarrow$ 2B	19	0.5%
No DMARC $\rightarrow$ 2A	3	0.1%
Total	4069	100%

TABLE V
DISTRIBUTION OF THE LAST TRANSITIONS TO 4B AT THE END OF THE OBSERVATION PERIOD. NOTE: THESE VALUES ALSO INCLUDE DOMAINS THAT UNDERWENT FURTHER TRANSITIONS BEFORE THIS FINAL CHANGE.

4B as end configuration	Count	%
1B $\rightarrow$ 4B	810	37.5%
3B $\rightarrow$ 4B	792	36.7%
No DMARC $\rightarrow$ 4B	402	18.6%
1A $\rightarrow$ 4B	61	2.8%
4A $\rightarrow$ 4B	49	2.3%
2B $\rightarrow$ 4B	32	1.5%
3A $\rightarrow$ 4B	13	0.6%
2A $\rightarrow$ 4B	1	0.0%
Total	2160	100.0%

E. Analysis of invalid DMARC entries

For the analysis of most common errors in invalid DMARC records, we focused on the 625 domains identified in our first sample on 2025-04-01. The identified error categories can be seen in VII. For each record, we employed the *checkdmarc* library, reporting only the first error encountered during parsing of the record. The first step in parsing the record was a comparison of the record against the grammar defined in the RFC. In 162 cases (25.9% of the invalid records) at least one violation of the formal syntax was present, which makes the record ineligible for further processing. The most frequent cause was the incorrect separation of tags: the RFC requires semicolons (";"), yet many records used spaces or commas as separators. Two domains (0.3%) lacked the mandatory policy definition via the *p* tag. A further 72 domains (11.5%) failed to respect the required order that the *p* tag must immediately follow the *v* tag. 27 domains (4.3%) contained tags that are not defined in the standard, including obvious typographical errors (e.g., "rfu" instead of "rua", "prct" instead of "pct") or completely unrelated tag names. The *fo* or *rf* tags were also problematic for 26 domains (4.2%). For example, for the report format, the value "iodef" was used where the RFC permits only "afrf". Eleven domains (1.8%) specified a *p* tag value outside the accepted set *none*, *quarantine*, *reject*, frequently due to misspellings ("non", "rnone", "quarantinei") or the inclusion of multiple values ("reject/quarantine"). A single domain (0.2%) listed a non numeric value for the *pct*-tag. Among the remaining domains, 202 (32.3%) contained errors related to the *rua*/*ruf* reporting URI: the most common

TABLE VI
MOST FREQUENT TRANSITION SEQUENCES BETWEEN DMARC CONFIGURATIONS OVER THE ENTIRE PERIOD. ABSOLUTE NUMBER AND RELATIVE PERCENTAGE IN RELATION TO THE NUMBER OF DOMAINS WITH TRANSITIONS.

Transition sequence					Count	%
No DMARC	→			1A	1052	9.9%
1B	→			3B	1029	9.7%
No DMARC	→			1B	984	9.2%
1B	→			4B	647	6.1%
No DMARC	→			3B	417	3.9%
3B	→			4B	412	3.9%
1A	→			1B	350	3.3%
No DMARC	→			4B	290	2.7%
1B	→			No DMARC	204	1.9%
1B	→	3B	→	4B	195	1.8%
1A	→			No DMARC	187	1.8%
No DMARC	→	3B	→	No DMARC	185	1.7%
1B	→	No DMARC	→	1B	175	1.6%
No DMARC	→	4B	→	No DMARC	159	1.5%
No DMARC	→			4A	132	1.2%
No DMARC	→			3A	124	1.2%
1A	→			3B	114	1.1%
1B	→			1A	112	1.1%
1B	→	2B	→	3B	91	0.9%
3B	→			1B	91	0.9%
1A	→			3A	89	0.8%
3B	→			No DMARC	80	0.8%
1B	→	3B	→	1B	80	0.8%
1A	→	No DMARC	→	1A	78	0.7%
2B	→			3B	78	0.7%
1B	→			2B	78	0.7%
4B	→			No DMARC	75	0.7%
4B	→			1B	73	0.7%
No DMARC	→	1B	→	3B	69	0.7%
3B	→	No DMARC	→	3B	68	0.6%
1A	→			4A	68	0.6%

TABLE VII
BREAKDOWN OF DOMAINS WITH INVALID DMARC RECORDS ON 2025-04-01 BY ERROR CATEGORIES

Error level	Count
Invalid DMARC records in total	625
—— Formal syntax	162
— —— No p-tag specified	2
— — —— p-tag does not follow v-tag	72
— — — —— Undefined tags	27
— — — — —— Invalid fo- / rf-tag value	26
— — — — — —— Invalid p-tag value	11
— — — — — — —— Invalid pct-tag value	1
— — — — — — — —— Invalid rua- / ruf-tag value	202
— — — — — — — — —— MX lookup failure	122

mistake was the omission of the "mailto:" statement, or the provision of invalid email addresses. The last 122 domains (19.5%) contained syntactically correct URIs, but the MX lookup for the reporting domain failed, causing report delivery impossible.

In summary, a variety of faults can invalidate a DMARC record, but the most prevalent issues are incorrect separation of tags and the provision of invalid reporting URIs.

F. Summary

Applying our proposed configuration matrix to real-world data reveals that 13.1% already use the target configuration 4B we defined in Section VI-A. The target configuration also saw the greatest increase (1.7 percentage points) over the observation period, while DMARC adoption in general grew by 2.8 percentage points (Section VI-B). Analysis of the transitions between first and last sample (Section VI-C) and on a daily basis (Section VI-D) showed that the most common paths taken to reach our target configuration 4B is, e.g., 1B → 3B → 4B. Lastly, our analysis of invalid records (Section VI-E) reveals that incorrect separation of tags and invalid reporting URIs are the most common errors present in our sample.

VII. DISCUSSION

In this work, we proposed a configuration matrix to classify real-world DMARC configurations. Compared to previous work, this also covers the pct and sp tags, giving a complete picture of their anti-spoofing effectiveness. We have defined a total of eight different configurations that differ in terms of their effectiveness in protecting against email spoofing. Based on our configuration matrix, we provide recommendations for both an initial (1B) and a target configuration (4B). While the initial configuration (1B) is recommended to test the DMARC implementation and detect potential issues, each domain owner should implement DMARC with sp and p = *reject*, pct = 100, and reporting enabled (4B) to achieve the greatest protection against spoofing.

Applying our configuration matrix to the Tranco Top 100k domains reveals that only 13.1% have the recommended target configuration (4B). If we only look at the number of domains that have p = *reject*, like Tatang et al. [16], or a combination of p = *reject* and rua/ruf set, like Hureau et al [27], our sample would yield 16.1% and 14.4% "effective" configurations, respectively. This indicated that their requirements also cover configurations that are in practice not as effective because they did not take all DMARC parameters, especially sp and pct, into account. Our proposed configuration matrix therefore draws a better picture of the actual effectiveness of DMARC configurations and helps to better understand the adoption of effective DMARC configurations in the future.

Tracking DMARC configurations over 8 months showed an increase of 2.8 percentage points in valid DMARC records, and allowed us to gain insight into the practical application of DMARC and to evaluate our recommended configurations Our recommended target configuration saw an increase of 1.7 percentage points compared to 1.1 percentage points for other DMARC configurations.

To better understand the implementation approaches and transitions between configurations used in practice, we performed daily scans. This revealed that most domains that underwent a change only changed their configuration once or twice, usually to a stronger configuration. After the initial configuration with 1A or 1B, we usually observe a transition to 3B, followed by 4B or from 1B to 4B directly. Thus, many domains are already following the configurations we recommend: Initially starting with p = *none* and reporting enabled (1B) but aiming for p = *reject* and reporting enabled

(4B). Unfortunately, many domains initially start with configuration 1A, which we do not recommend, as it ignores the reporting, which is an important aspect of DMARC and especially beneficial during initial setup. The only advantage of using 1A as a configuration is that a DMARC entry exists, thus fulfilling potential requirements of the receiving email server, as currently exist for Google, Yahoo, or Microsoft [6]. Another configuration we observed quite often is 3B, which offers no real benefit compared to 4B but enforces a weaker policy. Also, we see transitions from "no DMARC" to 3B and back to "no DMARC", probably due to too many false positives. This indicates that the different policy settings are not well understood, as prior work has already noted [27], [15].

An analysis of the most common DMARC errors in our sample confirms this. The most common error is a missing "mailto" in the rua/ruf tag and other issues that could be easily prevented by using one of the many (freely available) DMARC checkers. Additionally, we suspect that the pct tag is often misunderstood. We based our results on the current RFC 7489 [11]. A new draft[2] is currently under development, addressing some shortcomings, e.g., removing the pct tag. Unfortunately, it is not currently planned to define it as a new version (v=DMARC2) [27]. Therefore, it is unlikely that these changes will have an impact in the near future, given how long it took to reach the current level of adoption. We assume that most of these problems could be solved by providing clear recommendations for domain owners, such as those provided in our configuration matrix, and by identifying misunderstandings.

A. Limitations

In this paper, we adopt the specifications outlined in the relevant RFC and, for the purposes of our analysis, treat any deviation from the RFC as a criterion for classifying a DMARC record as invalid. While this offers a clear, reproducible rule, it might differ from real-world email-server behavior. Further, DMARC records are distributed via DNS, making them susceptible to attacks such as DNS poisoning. This limitation is inherent to DMARC. The use of protective measures, such as DNSSEC, to secure DNS is advisable but beyond the scope of this work. Our sample is based on the Tranco Top 100k list of domains and is therefore globally diverse, covering a wide range of countries and industries. However, related work has shown that DMARC adoption is higher among high-ranked domains [22], [16], suggesting that adoption rates and findings for our sample may not be representative of *all* domains worldwide. We lack complete data on national or sectoral DMARC awareness and information campaigns, so we cannot link changes in DMARC adoption to such efforts. The observed trend is linear, showing no sharp spikes that would indicate large, time-limited awareness campaigns.

[2]https://datatracker.ietf.org/doc/draft-ietf-dmarc-dmarcbis/

B. Future Work

The results of our work point to several interesting research directions that were out of scope for this work but could further deepen the understanding of real-world DMARC deployment. Firstly, extending the analysis to other samples (i.e., country- or industry-specific) would enable an assessment of how DMARC adoption differs from the large, global Tranco sample investigated here. A smaller sample would also allow for a more in-depth per-domain investigation of transitions. Secondly, a systematic exploration of how to inform domain owners with insecure configurations about the correct implementation of DMARC could deliver insights for improving adoption rates. Specifically, large-scale notification campaigns could identify domain owners' mental models or misunderstandings. Thirdly, while our daily scans provide a good overview of current real-world DMARC usage, the underlying reasons for opting out or for selecting particular configuration settings remain unexplored. Specifically, reasons to regress in configuration cannot be explained solely by our data analysis. Addressing these points using qualitative research would help inform the design of targeted awareness campaigns to encourage broader adoption and the secure deployment of DMARC among domain owners.

VIII. Conclusion

In this paper, we analyze DMARC adoption and configurations based on a new, utility-oriented configuration matrix. We provide clear recommendations for initial and target configurations based on our proposed matrix. The results of our daily sample over a duration of eight months show that our recommended configurations, 1B and 4B, are the most common ones, and the percentage of the domains with the target configuration, 4B, sees the greatest increase, from 13.1% to 14.8%. Looking at the configuration changes on a per-domain level over the observation period reveals that most configurations were changed to a stricter policy, increasing the effectiveness against email spoofing. For a deeper understanding, we looked at the transition sequences for domains. This gives us insights into how domains start out when initially configuring DMARC, revealing potential incorrect understanding of DMARC. 1% of domains with a DMARC record had an invalid record. Further investigations reveal that most issues are caused by syntactical errors and invalid URIs. A new version of the DMARC specification is currently in development addressing some of the issues found, but not solving the issue that most domains still use ineffective DMARC configurations. Continued measurement and improving DMARC configurations will remain an important task to fight against email spoofing and phishing attacks. We hope to improve the process of identifying and evaluating the state of DMARC adoption in the future with our proposed, utility-oriented configuration matrix and by providing our scanning tool as open source software.

Data Availability

To ensure reproducibility, all data and code used in this study are available in the following open-access repositories:

1) Code on Github: https://github.com/SecUSo/dmarc-configuration-analysis-madweb-2026 (commit 6354daa)
2) Data on OSF: https://doi.org/10.17605/OSF.IO/DSFZW

Acknowledgment

This research is supported by funding from the topic Engineering Secure Systems, topic 46.23.01 Methods for Engineering Secure Systems, of the Helmholtz Association (HGF) and by KASTEL Security Research Labs.

References

[1] "Simple Mail Transfer Protocol," RFC 821, Aug. 1982. [Online]. Available: https://www.rfc-editor.org/info/rfc821

[2] B. M. Berens, F. Schaub, M. Mossano, and M. Volkamer, "Better Together: The Interplay Between a Phishing Awareness Video and a Link-centric Phishing Support Tool," *Proceedings of the CHI Conference on Human Factors in Computing Systems*, pp. 1–60, 2024.

[3] J. Klütsch, J. Schwab, C. Böffel, V. Zimmermann, and S. J. Schlittmeier, "Friend or phisher: how known senders and fear of missing out affect young adults' phishing susceptibility on social media," *Humanities and Social Sciences Communications*, vol. 11, 2024.

[4] Google, "Phishing activity trends report 4th quarter 2024," https://docs.apwg.org/reports/apwg_trends_report_q4_2024.pdf, 2025, [Accessed 17-12-2025].

[5] H. Zhang, L. Chen, M. Liu, Y. Shi, S. Wu, and Z. Xue, "Both sides needed: A two-dimensional measurement study of email security based on SPF and DMARC," *2023 19th International Conference on Mobility, Sensing and Networking (MSN)*, vol. 00, pp. 855–861, 2023.

[6] Dmarcian, "Understanding gmail and yahoo dmarc requirements," https://dmarcian.com/yahoo-and-google-dmarc-required/, 2024, [Accessed 05-12-2025].

[7] D. Kondo, Y. Shibuya, R. S. Yamaguchi, T. Ishihara, Y. Sekiya, T. Nakata, and T. Asami, "Who did not implement email security measures after google's new email sender guidelines?: A large-scale measurement study," *2025 9th Network Traffic Measurement and Analysis Conference (TMA)*, vol. 00, pp. 1–10, 2025.

[8] S. Kitterman, "Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1," RFC 7208, Apr. 2014. [Online]. Available: https://www.rfc-editor.org/info/rfc7208

[9] M. Kucherawy, "Email Authentication Status Codes," RFC 7372, Sep. 2014. [Online]. Available: https://www.rfc-editor.org/info/rfc7372

[10] M. Kucherawy, D. Crocker, and T. Hansen, "DomainKeys Identified Mail (DKIM) Signatures," RFC 6376, Sep. 2011. [Online]. Available: https://www.rfc-editor.org/info/rfc6376

[11] M. Kucherawy and E. Zwicky, "Domain-based Message Authentication, Reporting, and Conformance (DMARC)," RFC 7489, Mar. 2015. [Online]. Available: https://www.rfc-editor.org/info/rfc7489

[12] Yahoo, "Faq sender hub dashboard," https://senders.yahooinc.com/faqs/, n.d., [Accessed 16-12-2025].

[13] Google, "Requirements for email senders," https://support.google.com/a/answer/81126, n.d., [Accessed 16-12-2025].

[14] Microsoft, "Strengthening email ecosystem: Outlook's new requirements for high-volume senders," https://techcommunity.microsoft.com/blog/microsoftdefenderforoffice365blog/strengthening-email-ecosystem-outlooks-new-requirements-for-highvolume-senders/4399730, 2025, [Accessed 16-12-2025].

[15] H. Hu, P. Peng, and G. Wang, "Towards understanding the adoption of anti-spoofing protocols in email systems," *2018 IEEE Cybersecurity Development (SecDev)*, pp. 94–101, 2018.

[16] D. Tatang, F. Zettl, and T. Holz, "The evolution of DNS-based email authentication: Measuring adoption and finding flaws," *24th International Symposium on Research in Attacks, Intrusions and Defenses*, pp. 354–369, 2021.

[17] H. Zhang, D. Mi, L. Chen, M. Liu, Y. Shi, and Z. Xue, "Subdomain protection is needed: An SPF and DMARC-based empirical measurement study and proactive solution of email security," *2023 42nd International Symposium on Reliable Distributed Systems (SRDS)*, vol. 00, pp. 140–150, 2023.

[18] M. I. Ashiq, W. Li, T. Fiebig, and T. Chung, "You've got report: Measurement and security implications of DMARC reporting," in *32nd USENIX Security Symposium (USENIX Security 23)*. Anaheim, CA: USENIX Association, 2023, pp. 4123–4137. [Online]. Available: https://www.usenix.org/conference/usenixsecurity23/presentation/ashiq

[19] B. Blechschmidt and B. Stock, "Extended hell(o): A comprehensive large-scale study on email confidentiality and integrity mechanisms in the wild," in *32nd USENIX Security Symposium (USENIX Security 23)*. Anaheim, CA: USENIX Association, 2023, pp. 4895–4912. [Online]. Available: https://www.usenix.org/conference/usenixsecurity23/presentation/blechschmidt

[20] dmarc.org, "Statistics - dmarc," https://dmarc.org/stats/dmarc/, n.d., [Accessed 07-12-2025].

[21] Z. Durumeric, D. Adrian, A. Mirian, J. Kasten, E. Bursztein, N. Lidzborski, K. Thomas, V. Eranti, M. Bailey, and J. A. Halderman, "Neither snow nor rain nor MITM..." *Proceedings of the 2015 Internet Measurement Conference*, pp. 27–39, 2015.

[22] M. Yajima, D. Chiba, Y. Yoneya, and T. Mori, "Measuring adoption of DNS security mechanisms with cross-sectional approach," *2021 IEEE Global Communications Conference (GLOBECOM)*, vol. 00, pp. 1–6, 2021.

[23] D. Pranić, "Analysis of DMARC implementation in republic of croatia," *2023 46th MIPRO ICT and Electronics Convention (MIPRO)*, vol. 00, pp. 1219–1224, 2023.

[24] D. Arnaldy and R. P. Theyser, "Analysis of apilogy.id email domain security status using DMARC (domain-based message authentication, reporting, and conformance)," *2023 6th International Conference of Computer and Informatics Engineering (IC2IE)*, vol. 00, pp. 125–130, 2023.

[25] S. Maroofi, M. Korczyński, A. Hölzel, and A. Duda, "Adoption of email anti-spoofing schemes: A large scale analysis," *IEEE Transactions on Network and Service Management*, vol. 18, no. 3, pp. 3184–3196, 2021.

[26] V. Dakić, Z. Morić, M. Šepić, and A. Kapulica, "Evaluating e-mail domain protection system adoption by croatian financial institutions," *2025 10th International Conference on Cloud Computing and Big Data Analytics (ICCCBDA)*, vol. 00, pp. 1–10, 2025.

[27] O. Hureau, J. Bayer, A. Duda, and M. Korczyński, "Spoofed emails: An analysis of the issues hindering a larger deployment of DMARC," *Lecture Notes in Computer Science*, pp. 232–261, 2024.

[28] Bundesamt für Sicherheit in der Informationstechnik (BSI), "BSI Technical Guideline TR-03182: E-Mail Authentication – Methods for Sender Identification," Bundesamt für Sicherheit in der Informationstechnik (BSI), Tech. Rep., 2023. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03182/BSI-TR-03182.pdf

[29] V. Le Pochat, T. Van Goethem, S. Tajalizadehkhoob, M. Korczyński, and W. Joosen, "Tranco: A research-oriented top sites ranking hardened against manipulation," in *Proceedings of the 26th Annual Network and Distributed System Security Symposium*, ser. NDSS 2019, Feb. 2019.