Coremail论客

A Large-scale and Longitudinal Measurement Study of DKIM Deployment

Chuhan Wang, Kaiwen Shen, Minglei Guo, Yuxuan Zhao, Mingming Zhang, Jianjun Chen, Baojun Liu, Xiaofeng Zheng, Haixin Duan, Yanzhong Lin, Qingfeng Pan

Email: wch22@mails.tsinghua.edu.cn

What is DKIM?

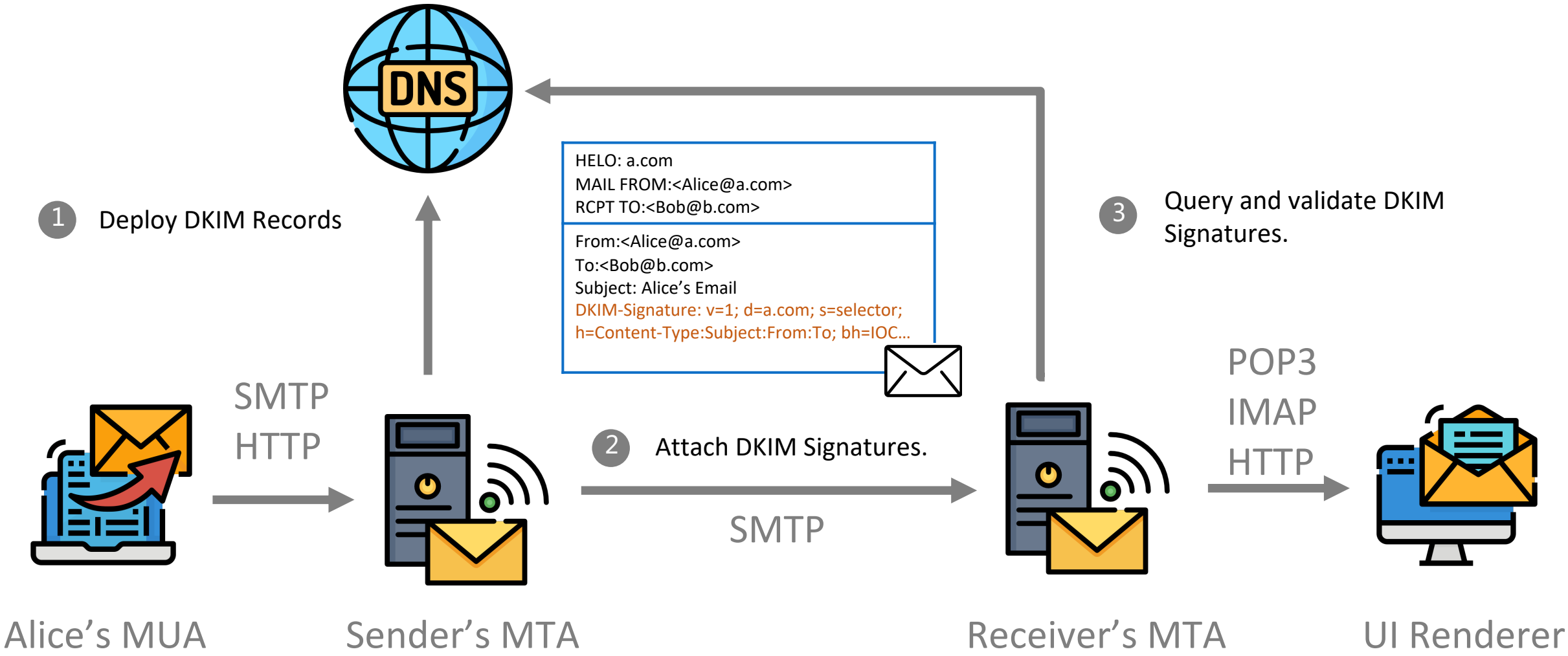
DomainKeys Identified Mail (DKIM) is an email authentication protocol, based on the digital signatures. It is designed to prevent emails from being forged or tampered within transit.

<selector>._domainkey.*<example.com>*

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
s=selector; d=example.com; h=From:To:Subject; l=200;
bh=vYFvy46eesudgj4s…; b=IHEFQ+7rcisqsRBSEdd83…

An Example of DKIM Signature Header.

The Workflow of DKIM



How to Measure DKIM Deployment

Metric	*Alexa Hosts*	*Adobe Hosts*	*Adobe Users*
DNSSEC	3.40%	2.75%	4.92%
Valid	2.96%	2.12%	1.35%
Invalid	0.44%	0.63%	3.57%
DMARC	0.97%	0.90%	67.81%
None	0.73%	0.66%	51.29%
Quarantine	0.08%	0.06%	0.46%
Reject	0.16%	0.18%	16.06%
SPF	42.26%	43.60%	85.02%

Table 8: DNSSEC, DMARC and SPF status of the Alexa and Adobe top million hosts.

CCS 2015[1]

Status	All Domain # (%)	MX Domain # (%)
Total domains	1,000,000 (100%)	792,556 (100%)
w/ SPF	492,300 (49.2%)	473,457 (59.7%)
w/ valid SPF	**448,741 (44.9%)**	**430,504 (54.3%)**
Policy: soft fail	272,642 (27.3%)	268,317 (33.9%)
Policy: hard fail	**125,245 (12.5%)**	**112,415 (14.2%)**
Policy: neutral	49,798 (5.0%)	48,736 (6.1%)
Policy: pass	1,056 (0.1%)	1,036 (0.1%)
w/ DMARC	51,222 (5.1%)	47,737 (6.0%)
w/ valid DMARC	**50,619 (5.1%)**	**47,159 (6.0%)**
Policy: none	39,559 (4.0%)	36,984 (4.7%)
Policy: reject	**6,016 (0.6%)**	**5,225 (0.7%)**
Policy: quarantine	5,044 (0.5%)	4,950 (0.6%)

Table 1: SPF/DMARC statistics of Alexa 1 million domains. The data was collected in January 2018.

USENIX 2018[2]

DKIM Records

↓

<selector>._domainkey.example.com

↓

Passive DNS Datasets

奇安信 360

DKIM Signatures

↓

Only exist in the email headers

↓

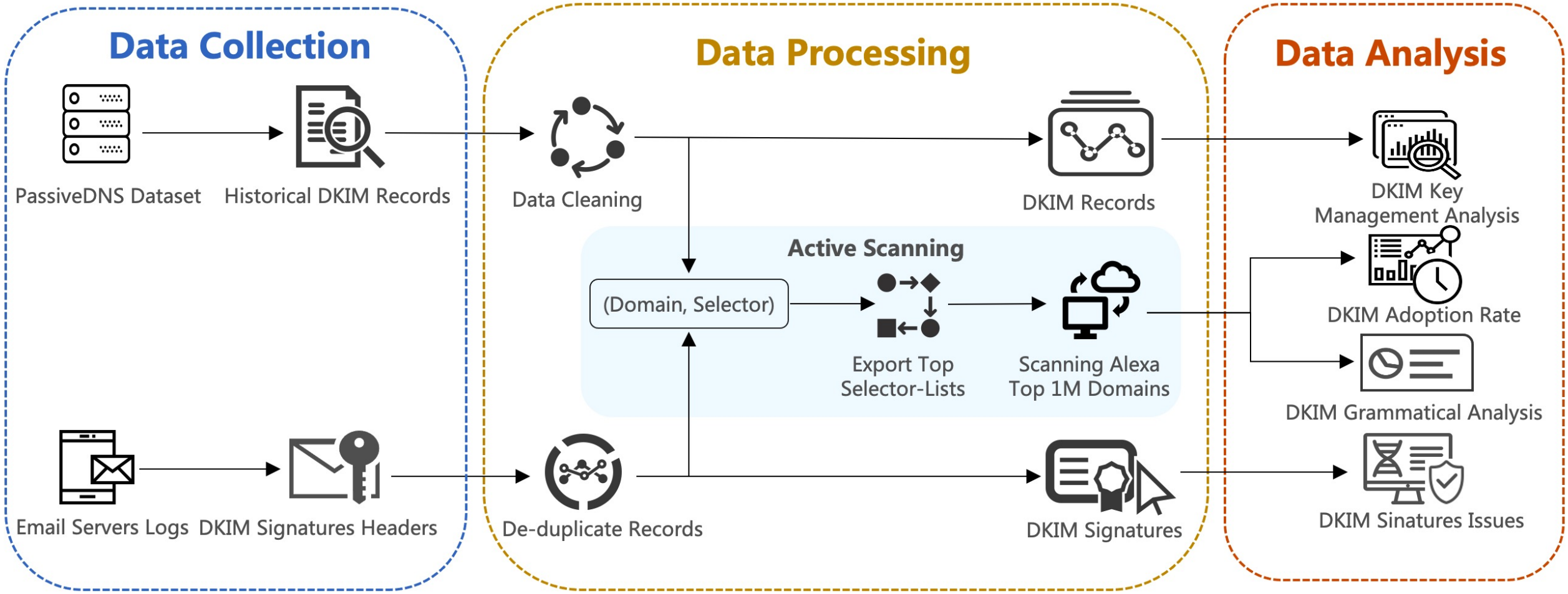
Email Server Logs

Coremail 论客

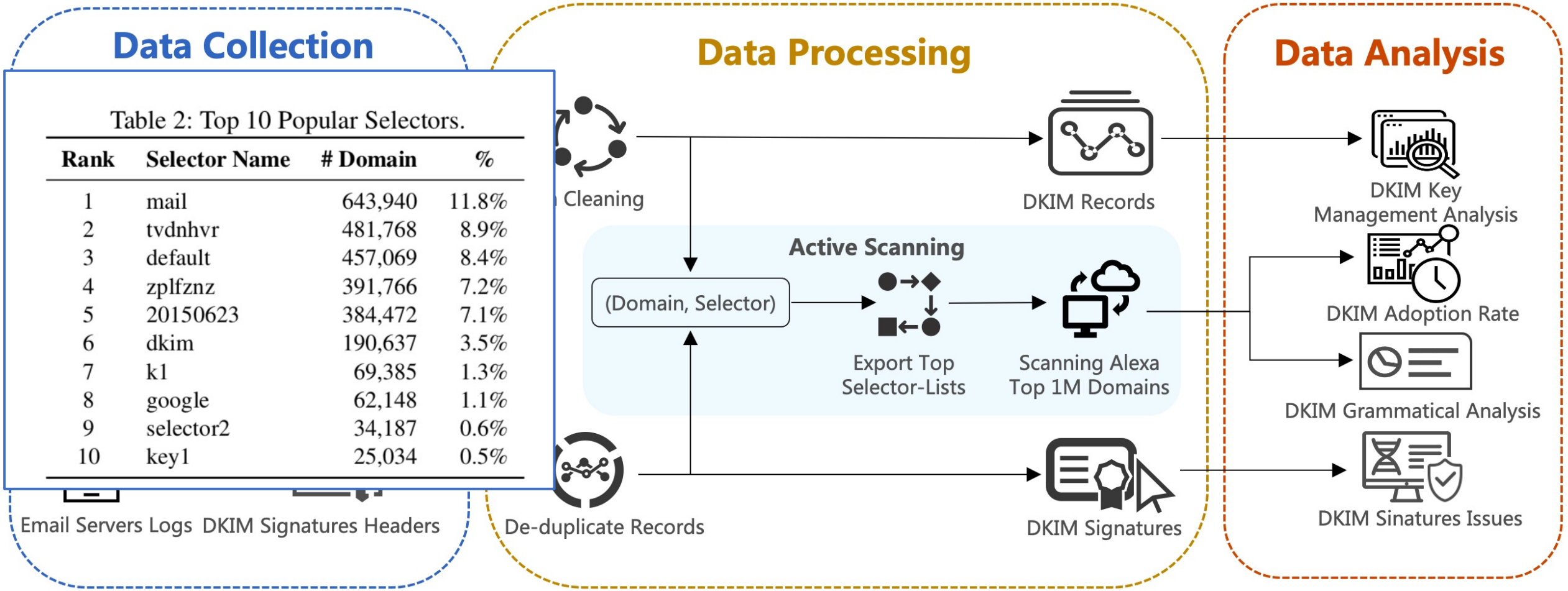
Our passive collection data is the combination of the above two parts and includes **5,448,169** distinct domains and **2,376,077** selectors in total.

[1] Security by Any Other Name: On the Effectiveness of Provider Based Email Security (CCS 2015)
[2] End-to-End Measurements of Email Spoofing Attacks (USENIX 2018)

Overview of DKIM Data Collection and Analysis

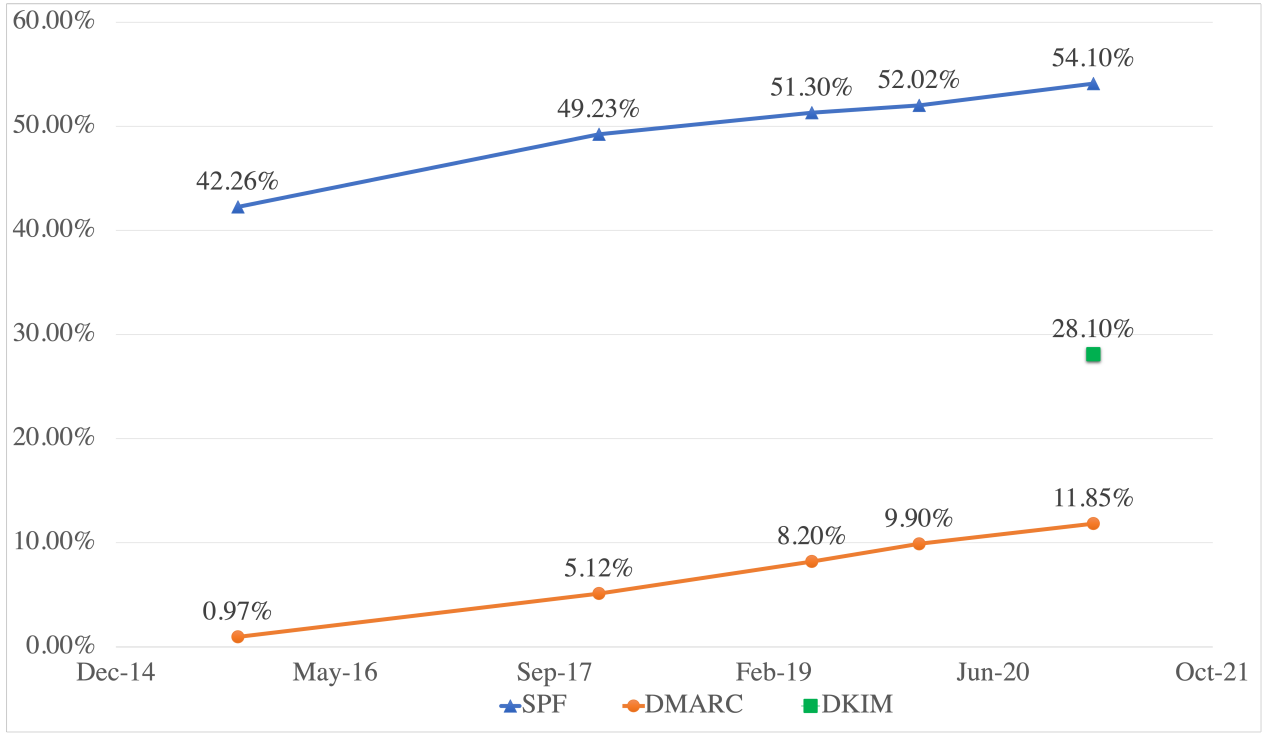


Overview of DKIM Data Collection and Analysis



The Adoption Rate of SPF/DKIM/DMARC

The result shows that **28.1%** of Alexa Top 1 Million domains have enabled DKIM, of which **2.9%** are misconfigured.



The Adoption Rate of SPF/DKIM/DMARC in Alexa Top 1M Domains[1,2]

Table 5: DKIM Adoption Rate among Multiple gTLDs.

gTLD	MX Domains	w/ DKIM (%)
.com	371,040	143,156 (38.6%)
.org	33,271	13,787 (41.4%)
.net	33,101	9,926 (30.0%)
.info	5,531	1,443 (26.1%)
.co	3,559	1,453 (40.8%)
.edu	3,062	2,183 (71.3%)
.biz	1,955	534 (27.3%)
.gov	810	431 (53.1%)

Table 6: DKIM Adoption Rate among Multiple ccTLDs.

ccTLD	Country	MX Domains	w/ DKIM (%)
.ru	Russia	34,754	12,107 (34.8%)
.de	Germany	25,105	5,744 (22.9%)
.jp	Japan	17,740	2,467 (13.9%)
.uk	United Kingdom	15,496	7,058 (45.6%)
.br	Brazil	13,990	6,737 (48.2%)
.fr	France	11,012	4,141 (37.6%)
.au	Australia	7,452	4,363 (58.6%)
.cn	China	5,439	422 (7.8%)

[1] Security by Any Other Name: On the Effectiveness of Provider Based Email Security (CCS 2015)
[2] End-to-End Measurements of Email Spoofing Attacks (USENIX 2018)

DKIM Key Management Issues

Long Lifetime Keys

RFC 6376 recommends that, DKIM keys should be rotated on a routine basis to balance the security risk of compromised keys and operational effort. However, we find using long-lifetime keys is common even for the most high-profile domains.

We find **10** out of Alexa top 20 domains have not rotated their keys in the past 5 years, while the percentage is **68.5%** out of Alexa top 100 domains[1].

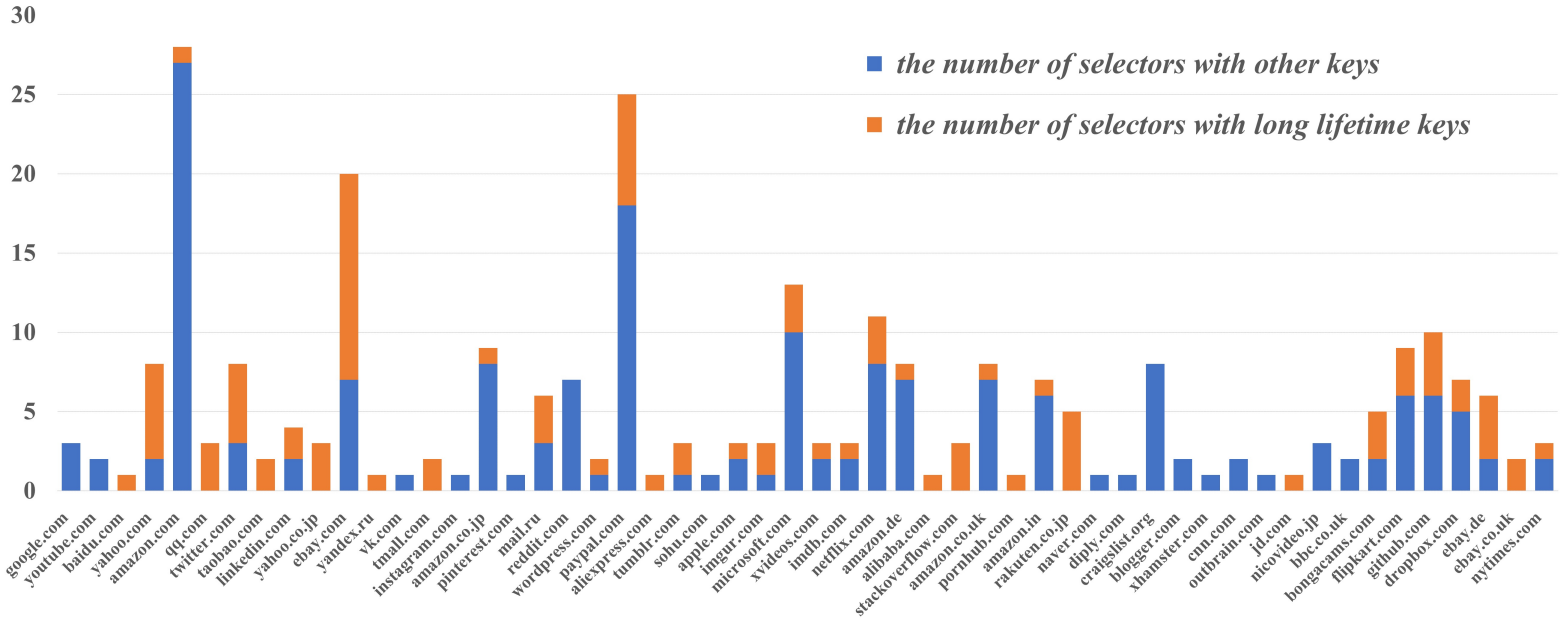


Table 8: DKIM Key Lifetime in Passive DNS Dataset

DKIM Key Lifetime(year)	# Domain	%
≥ 1	793,679	21.9%
≥ 2	652,742	18.0%
≥ 3	521,033	14.4%
≥ 4	414,022	11.4%
≥ 5	312,852	8.6%

[1] The number of domains with long lifetime DKIM keys is a subset of those with short ones. For example, lifetime ≥ 2 is a subset of lifetime ≥ 1.

[1] The picture shows the number of long lifetime keys of 54 domains within Alexa top 100 covered by passive DNS data,

DKIM Key Management Issues

Weak Keys

RFC 8301 has pointed out that short RSA keys more easily succumb to off-line attacks and signers should use RSA keys of at least 2048 bits. NIST[1] has also recommended against using 1024-bit keys since December 31, 2013.

However, Our research finds **84%** of 3,631,768 domains still use the DKIM key of 1024 bits or less.

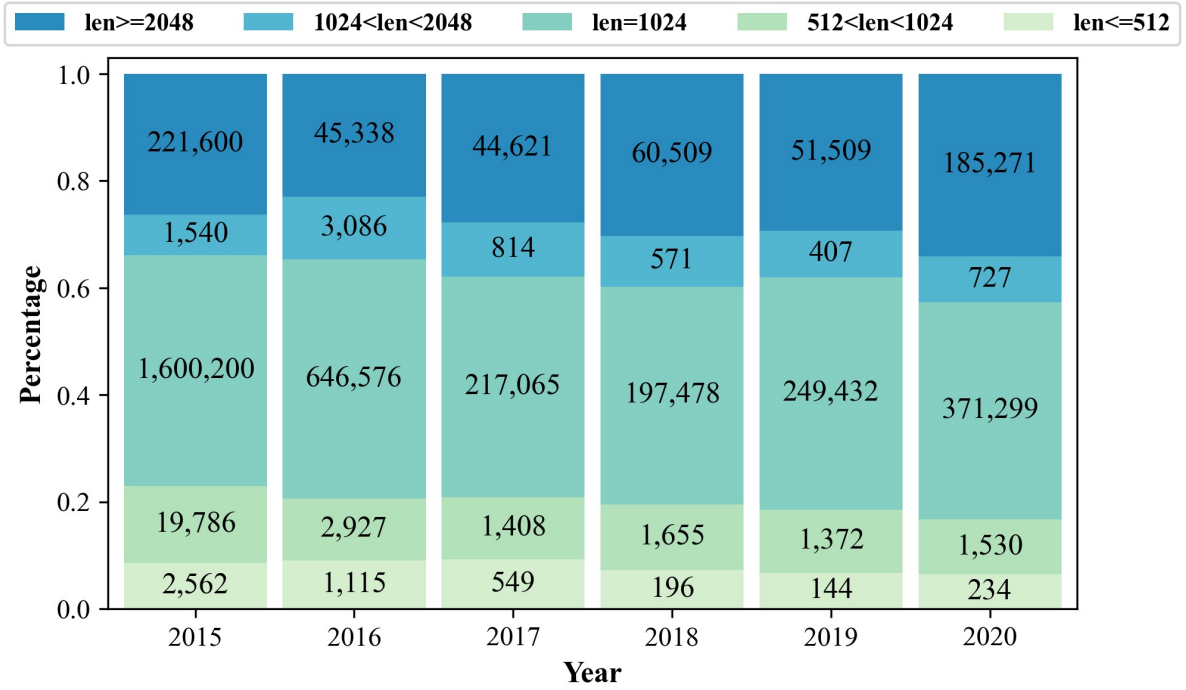


Table 10: DKIM Key Length in PassiveDNS.

DKIM Key Length	# Domain	%
$len = 2048$	579,032	16.0%
$1024 < len < 2048$	6,611	0.2%
$len = 1024$	3,006,398	82.9%
$512 < len < 1024$	30,431	0.8%
$len \leq 512$	5,399	0.2%

[1] National Institute of Standards and Technology

DKIM Signature Issues

Weak DKIM Signatures

DKIM signatures should sign some important email header fields to protect the content integrity of the email and avoid being abused for replay attacks. However, in RFC 6376, only the ***From*** field is specified to be ***MUST*** signed.

> *The basic rule for choosing fields to include is to select those 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; however, with these included, the core of the message is valid, even if sent on to new recipients.*

```
From (REQUIRED)
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
```

Table 12: Top 10 Email Headers in DKIM Signatures.

Rank	Field Name	%
1	From	100.0%
2	Subject	99.7%
3	To	86.7%
4	Date	75.8%
5	Mime-Version	73.6%
6	Message-Id	73.3%
7	Content-Type	67.5%
8	Content-Transfer-Encoding	19.5%
9	X-Ms-Exchange-Senderadcheck	12.5%
10	Reply-To	11.4%

DKIM Signature Issues

Oversigning

Oversigning means a header name should appear in “h=” tags once more than the actual number of that header in an email. The oversigning mechanism is helpful to protect users from the email spoofing attacks that use multiple email headers.

However, we found only **47549 (2.2%)** domains used oversigning mechanism.

```
DKIM-Signature: v=1; d=example.com; s=selector;
h=From:To:Subject:Content-Type:Reply-To:Date:Cc;
bh=IOC…
```

```
DKIM-Signature: v=1; d=example.com; s=selector;
h=From:From:To:To:Subject:Subject:Content-
Type:Content-Type:Reply-To:Reply-
To:Date:Date:Cc:Cc; bh=IOC…
```

An Example of Oversigning Mechanism

Table 13: Top 10 Headers Protected by Oversigning Mechanism.

Rank	Field Name	# Domain	%
1	From	47,334	99.5%
2	Subject	16,597	34.9%
3	Date	11,144	23.4%
4	To	5,913	12.4%
5	Message-Id	5,068	10.7%
6	In-Reply-To	2,611	5.5%
7	References	2,487	5.2%
8	Cc	2,004	4.2%
9	Reply-To	603	1.3%
10	Sender	165	0.3%

Mitigations

Mitigations

Disclosure

We have tried to responsibly report all vulnerabilities we found to the relevant email administrators.

4 email vendors and 24 relevant email administrators have acknowledged our report. Among them, Zoho.com provided us a reward of $200.

Online Detection Tool

Our tool can do the grammar check and analyze the key strength and judge whether the DKIM signatures have the security issues mentioned in this paper.

https://nospoofing.cn

Recommendations

DKIM Key Expiration Date

Adding an expired date for DKIM keys can help:

- alleviate the problem of the unclear transition period
- promote regular key replacement.

```
v=DKIM1; k=rsa; h=sha256;
p=MIGfMA0GCSqGSIb3DQCyOmR3diPVt1...
```

add a field of DKIM key expired time

```
v=DKIM1; k=rsa; h=sha256;
expired-date: Sun, 24 Jul 2022 10:28:34 GMT;
p=MIGfMA0GCSqGSIb3DQCyOmR3diPVt1...
```

Default Oversigning Mechanism

Setting oversigning as the default mechanism can help:

- improve the protective effect of DKIM signatures
- prevent DKIM signatures from being used for replay attacks.

```
DKIM-Signature: v=1; d=example.com; s=selector;
h=From:To:Subject:Content-Type:Reply-To:Date:Cc;
bh=IOC…
```

use default oversigning mechanism

```
DKIM-Signature: v=1; d=example.com; s=selector;
h=From:From:To:To:Subject:Subject:Content-
Type:Content-Type:Reply-To:Reply-
To:Date:Date:Cc:Cc; bh=IOC…
```

Q&A

Thanks for listening