VALIMAIL

DKIM L= Tag Exploit

Quick Overview
By Al Iverson

May 17, 2024

Agenda

- Email Authentication:
  SPF, DKIM, DMARC
- DKIM and How it Works
- The L= Tag / What is the Risk?
- What can bad guys do?
- May 17 Disclosure
- Who’s at Risk? How broad?
- How to Protect Yourself, Your Platform, and/or Your Customers

Email Authentication

a``

SPF

Sender Policy Framework – an email authentication setting for a domain that is essentially a list of IPs allowed to originate mail for that given email domain name.

Is based on IP addresses.

DKIM

DomainKeys Identified Mail – two cryptographic signatures are generated and stored in an email header. At receipt, these are validated using the public key to confirm messages were not altered in transit, and that the domain in question is the responsible party for the message.

Is NOT based on IP addresses.

DMARC

Domain-based Message Authentication and Conformance is the mechanism by which sending domains ask mailbox providers what to do with mail that fails authentication checks – often this means rejecting failed or unauthenticated mail.

DKIM Steps: Create, Transmit, Receive

a``

Create & Sign Message

Cryptographic signatures are created (and stored in email header of message) by mail server (MTA) at time of message creation. These “hashes” allow checking for content/header changes at receipt.

Transmit Message

Message transmitted from sending server to receiving server.

Receive & Check Signature

Message received by mailbox provider (i.e. Gmail, Hotmail, Yahoo). Mailbox provider checks signature using sending domain’s public key, confirms whether or not any of the protected elements have been modified since the message was created.

The L= Tag

What is the risk?

- The L tag is an optional DKIM configuration setting that LIMITS the number of characters into the body that the DKIM signature protects/affirms.
- General use by email senders generally does not need / should not use the L= tag, because of the limit to DKIM signature value.
- Original intent: Support mailing lists that might need to modify content / add an (email) signature.
- But even the RFC warns about significant risk.
  - See RFC 6376 section 8.2. See https://xnnd.com/csii
  - Learn more from our blog: https://xnnd.com/xwfm

What could bad guys do?

If you used L=(something) or L=1, bad guys could:

- Take your email message, add additional content to the end of it, or change the content beyond point X (whatever the L value is, in characters), re-inject that message via SMTP, and have that message still pass DKIM authentication.
- If L=1, this is even easier; we found this L= setting in the wild in some messages and it effectively means that the DKIM signature protects only the first character of the email message body – effectively no protection!
- Bad guys who didn’t think of this before will perhaps now be made aware of it due to broad recent disclosure.

Another big problem

Especially for affected marketers/ESPs

Receiving mailbox providers are going to treat L= tag containing email messages as unsigned.

- No DKIM means no compliance with new Yahoo/Google requirements.
- We believe Yahoo & Gmail are implementing this now or have already.
- IONOS 1&1 (GMX, mail.com, web.de+more) has already implemented this.
- We believe others are likely to follow suit.

May 17 2024 Disclosure

“BIMI and DMARC Can’t Save You: The Overlooked DKIM Exploit”

Disclosed by Estonian web-hosting and domain/mailbox provider ZONE: https://xnnd.com/qe2r

Exploit: “Replacing the boundary value in the Content-Type header in MIME multipart emails and adding a new MIME structure that uses the modified boundary at the end of the email. Such modification renders the existing MIME structure into a non-visible comment and forces the email client to treat the added structure as the “real” email content. This results in a larger impact and differs from other previously described approaches.”

- ZONE ties this exploit to DMARC and BIMI in their disclosure, but admits that the underlying issue is a looseness of interpretation of the DKIM email authentication protocol.
- Google, Apple and others have indicated that they have mitigated against this issue or that they plan to.

Who's at risk?

How broad is this?

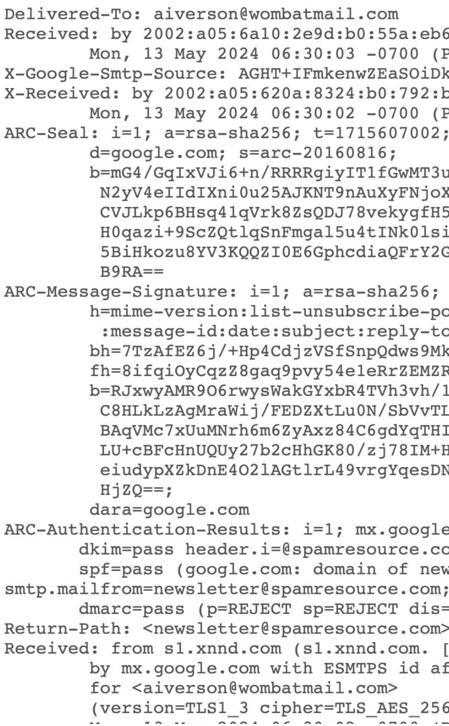
- The L= tag is not broadly used, if you consider it in the scope of % of email domains and volume of email messages sent daily.
- However, ZONE warned of observing exploitable messages referencing various Fortune 500 companies.
- Our sampling shows only a tiny number of messages affected, but...
  - At least one known email service provider platform incorporates the L= tag in all sends. We've notified them.
  - We have not identified any other well-known ESPs or marketing automation platforms affected (as of yet). We will notify any we find.
  - Keep in mind that you need to see a sent message's headers to identify this issue. It can't be queried via DNS.

Protection & Mitigation

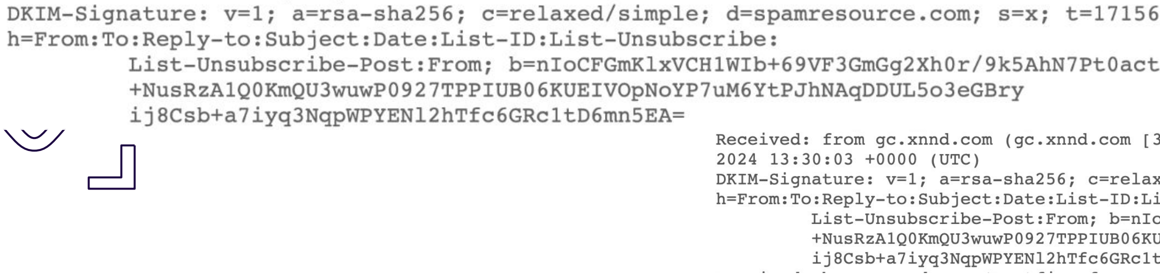
Mailbox Providers & ISPs	ESP/Marketing Platforms	Marketers/ Publishers
Remove support for L= tag in auth checks.	Modify DKIM configuration to remove L= tag.	Check headers; make sure DKIM signature doesn’t contain L= tag.
Gmail, Yahoo, 1&1 IONOS + more seem to be moving this way.	Rotate DKIM keys to ensure prior-signed messages no longer pass checks.	Check with your sending platform; ask them about DKIM config and key rotation.

Checking Headers

- View Source / Show Original
- Look for DKIM-Signature Header
- Confirm no “l tag” in header
- Or use tool like Steve Atkins’ Aboutmy.email



```
Delivered-To: aiverson@wombatmail.com
Received: by 2002:a05:6a10:2e9d:b0:55a:eb6
        Mon, 13 May 2024 06:30:03 -0700 (P
X-Google-Smtp-Source: AGHT+IFmkenwZEaSOiDk
X-Received: by 2002:a05:620a:8324:b0:792:b
        Mon, 13 May 2024 06:30:02 -0700 (P
ARC-Seal: i=1; a=rsa-sha256; t=1715607002;
        d=google.com; s=arc-20160816;
        b=mG4/GqIxVJi6+n/RRRRgiyIT1fGwMT3u
         N2yV4eIIdIXni0u25AJKNT9nAuXyFNjoX
         CVJLkp6BHsq41qVrk8ZsQDJ78vekygfH5
         H0qazi+9ScZQtlqSnFmgal5u4tINk0lsi
         5BiHkozu8YV3KQQZI0E6GphcdiaQFrY2G
         B9RA==
ARC-Message-Signature: i=1; a=rsa-sha256;
        h=mime-version:list-unsubscribe-po
         :message-id:date:subject:reply-to
        bh=7TzAfEZ6j/+Hp4CdjzVSfSnpQdws9Mk
        fh=8ifqiOyCqzZ8gaq9pvy54e1eRrZEMZR
        b=RJxwyAMR9O6rwysWakGYxbR4TVh3vh/1
         C8HLkLzAgMraWij/FEDZXtLu0N/SbVvTL
         BAqVMc7xUuMNrh6m6ZyAxz84C6gdYqTHI
         LU+cBFcHnUQUy27b2cHhGK80/zj78IM+H
         eiudypXZkDnE4O2lAGtlrL49vrgYqesDN
         HjZQ==;
        dara=google.com
ARC-Authentication-Results: i=1; mx.google
       dkim=pass header.i=@spamresource.co
       spf=pass (google.com: domain of new
smtp.mailfrom=newsletter@spamresource.com;
       dmarc=pass (p=REJECT sp=REJECT dis=
Return-Path: <newsletter@spamresource.com>
Received: from s1.xnnd.com (s1.xnnd.com. [
        by mx.google.com with ESMTPS id af
        for <aiverson@wombatmail.com>
        (version=TLS1_3 cipher=TLS_AES_256
```



```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=spamresource.com; s=x; t=17156
h=From:To:Reply-to:Subject:Date:List-ID:List-Unsubscribe:
         List-Unsubscribe-Post:From; b=nIoCFGmKlxVCH1WIb+69VF3GmGg2Xh0r/9k5AhN7Pt0act
         +NusRzA1Q0KmQU3wuwP0927TPPIUB06KUEIVOpNoYP7uM6YtPJhNAqDDUL5o3eGBry
         ij8Csb+a7iyq3NqpWPYENl2hTfc6GRc1tD6mn5EA=
```

```
Received: from gc.xnnd.com (gc.xnnd.com [3
2024 13:30:03 +0000 (UTC)
DKIM-Signature: v=1; a=rsa-sha256; c=relax
h=From:To:Reply-to:Subject:Date:List-ID:Li
         List-Unsubscribe-Post:From; b=nIo
         +NusRzA1Q0KmQU3wuwP0927TPPIUB06KU
         ij8Csb+a7iyq3NqpWPYENl2hTfc6GRc1t
```

Thank You.

Al Iverson, Industry Research and Community Engagement Lead
Email me: al.iverson@valimail.com