DKIM Replay: Problem and Possible Solutions

IETF 115 Dispatch
7 November 2022

Wei Chuang (weihaw@google.com), Bron Gondwana (brong@fastmailteam.com)

Email Authentication

- **Problem Statement**
- Proposals

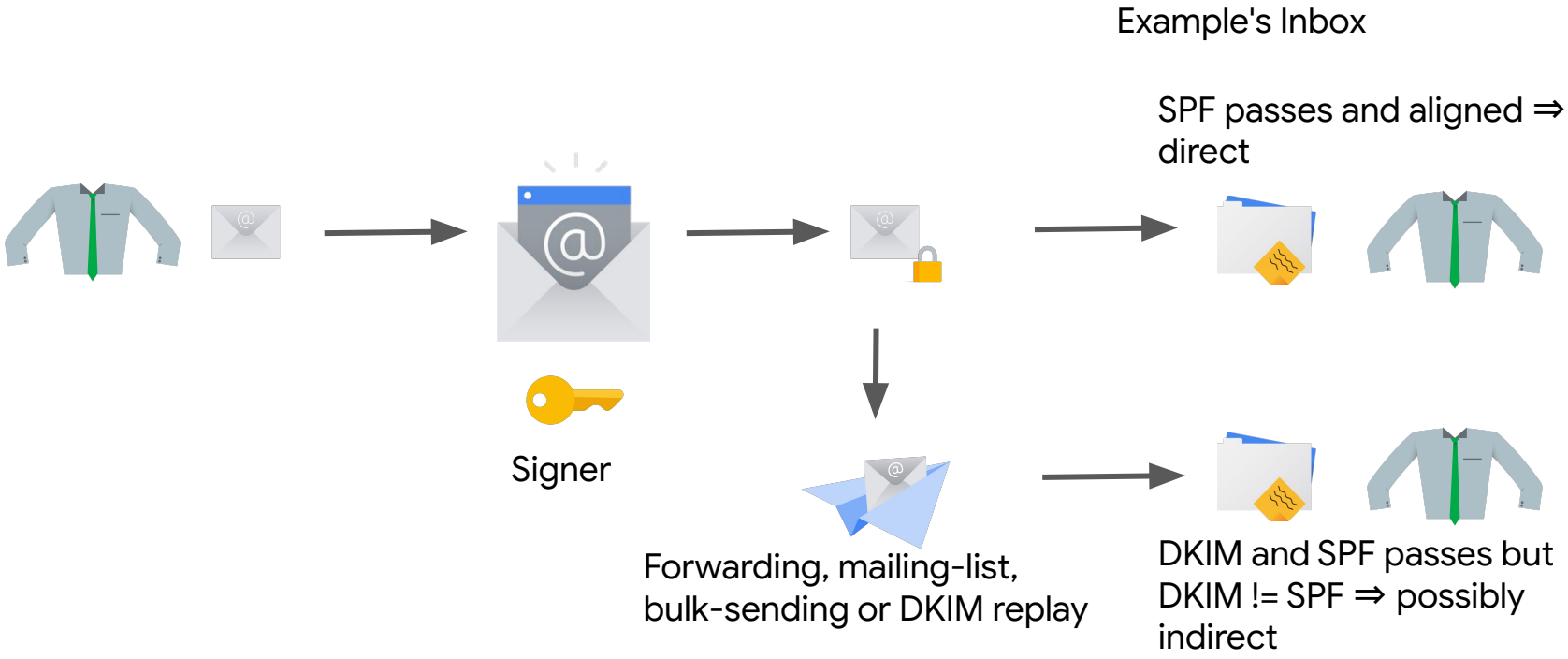
- **DKIM** RFC6376 is a mechanism to sign/authenticate an email. Recipient knows the signed parts were not modified after it was sent
- **SPF** RFC7208 is a mechanism to authenticate the sending mail server

- **DKIM Replay** (RFC6376 section 8.6) is a spam message sent through a well known DKIM signer to leverage the reputation of the signer. That signed spam message is then re-sent to many victim recipients, leveraging (and hurting) the signer's reputation.

Email Authentication ambiguity

- **Problem Statement**
- Proposals

- **DKIM != SPF could mean email was either auto-forwarded, sent by a mailing-list, or bulk sender, or DKIM replay.** It's hard distinguish the former benign cases from the later malicious one.



DKIM Replay Step 1: Spammer generates high-reputation signed email

- **Problem Statement**
- Proposals

- Spammer sends spam email from high-reputation domain to controlled account
- Email carries the sender DKIM signature and high-reputation
- Controlled account can recover email from spam folder

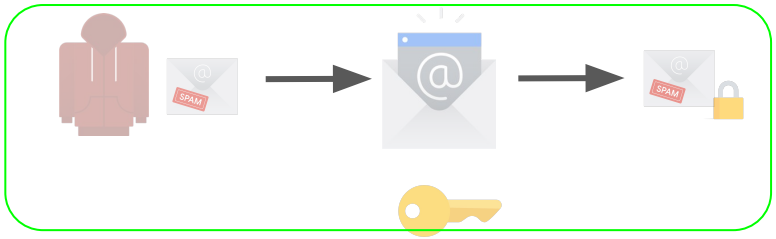
Signer

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=signer.com;
s=selector2; t=1649197869; bh=7J95C+c1pKK1U1bu+PVKr4dlwRXjOFQ4Cm7uj8/k0Zw=;
h=Date:From:Reply-To:Message-ID:From:Date:Reply-To:Feedback-ID:Message-ID;
b=j6KHopXulKBNaW96/ueVcQZ2iYhVrKdu7n+T1djeDSZkbhJqidBkFpP+XEi3vpnri
VNPe3F5Vg811oSHphBGt8iRLkb08wj61GJ3Y8ZSSZpNJdZlLkhdn4Whbb/R/f960Ha
ub5JAe7PErZp6TMn8rj4ET8M9oxBI62bXh2TqdjN5PzP+POKJKIo/YSA+EB5eaed4o
CTP2+JfQel4Sy/iMyoQNmVPkgXGytKvO76vaCE+T0Iplftn7blyXVzp4/LE58JXpdY
7QMPuxlJCsDc6E9ZELWi9dfN4Q4aTilg9VGvO2r4qRSyYe5nPIkwkUXW23Pr5OvcIc
HwlIVIFROgTZA==
```

DKIM Replay Step 2: Spammer amplifies email

- **Problem Statement**
- Proposals

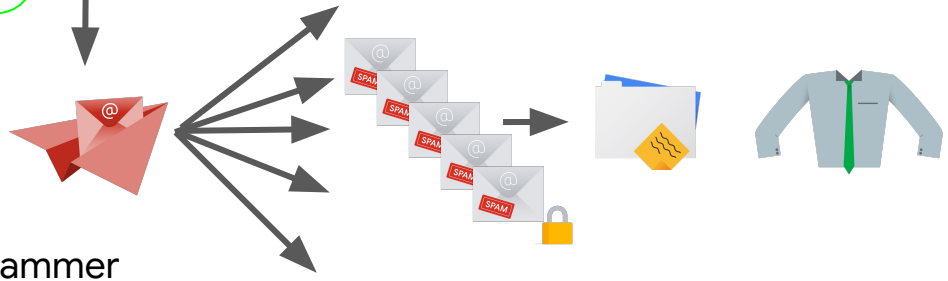
- Sends huge number of copies of each message using servers they control.
- Messages have *signer.com* DKIM authentication and *spammer.com* SPF authentication.
- Looking like forwarded Signer's messages ⇒ accepted by the spam filter.
  [**FN: spam gets through**]



Message sent from high-reputation signer.com account

```
DKIM-Signature: ....
To: "John Victim Doe" <john.doe@example.com>
Subject: You've won one millions dollars!

Please click here...
```

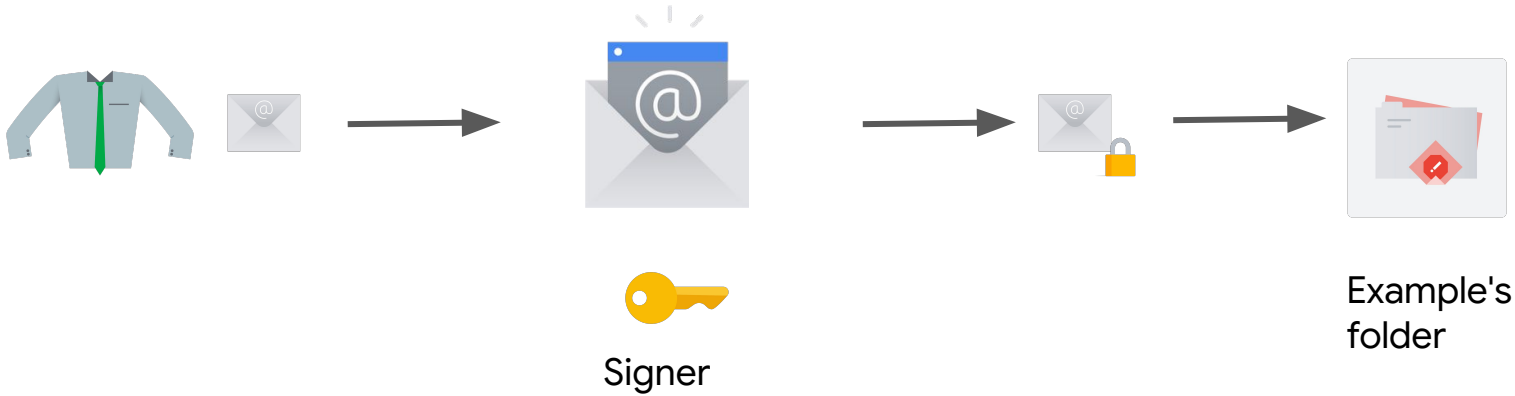


Spammer

DKIM replay step 3: Consequences

- **Problem Statement**
- Proposals

- Spam filters catch up with the influx of spam
- Signer's domain reputation drops.
  (On Gmail, use Postmaster tools to observe DKIM reputation changes)
- If the DKIM replay attack is large enough then deliverability of Signer will start being impacted.
  Since their reputation is low they are more likely to get caught by the spam system.
  [**FP: good mail gets caught**]



Proposals from DKIM Replay BoF

- Problem Statement
- **Proposals**

- At M3AAWG 56-Brooklyn, NY (12 Oct 2022)
- Drafts
  - draft-kucherawy-dkim-anti-replay
  - draft-chuang-replay-resistant-arc
  - draft-bradshaw-envelope-validation-extension-dkim
  - draft-gondwana-email-mailpath

- Problem statement: draft-chuang-dkim-replay-problem
  - Categorizes traffic flows especially w/forwarding
  - Taxonomy of four groups of solutions

Solutions 1/4: Recipient in the signature

- Problem Statement
- **Proposals**

- Proposed in:
  - draft-kucherawy-dkim-anti-replay
  - draft-bradshaw-envelope-validation-extension-dkim
  - draft-chuang-replay-resistant-arc
- Put envelope recipient identity in the DKIM signature
  - implicit address hash- draft-kucherawy-dkim-anti-replay
  - address hash in header- draft-bradshaw-envelope-validation-extension-dkim
  - explicit address in header- draft-chuang-replay-resistant-arc
- Avoids replay to destination addresses not anticipated by the DKIM signer
- Potentially indirect email flows impacted as badly as SPF (vs complexity)

Solutions 2/4: Count DKIM signatures

- Problem Statement
- **Proposals**

- Count messages by DKIM signatures, and filter above threshold
- Used by:
  - Yahoo (mentioned in BoF Q/A session)
- Mailing list traffic, exploder aliases, or regular BCCs will appear as duplicates and will get unintentionally get caught

Solutions 3/4: Strip DKIM signatures

- Problem Statement
- **Proposals**

- Sign and strip DKIM signatures per SMTP transaction on mailbox delivery
  - May separate a long term DKIM signature and per delivery signature
- Strawman (not known to be used)
- Doesn't help with evil mail server
- SPF like behavior again

Solutions 4/4: Gather per-hop signatures

- Problem Statement
- **Proposals**

- Per-hop signature and specify the next hop destination domain
  - Messages with this kind of signature cannot be replayed down a different pathway, since the destination won't match
  - Tolerates forwarding but
  - Additional signing overhead
- Proposed in:
  - draft-chuang-replay-resistant-arc
  - draft-gondwana-email-mailpath
- Requires every site along the path to support this spec, so it will need to detect whether the next stop is making a commitment to follow the spec.
  - If email goes outside of sites with this spec (without disclosure), traversing a naive forwarder remains indistinguishable from replay

What should we do?

- Problem Statement
- **Proposals**

- Spin up a new email authentication WG
  - Complement DMARC WG
- Goals
  - Authenticate messages to a sending domain
  - Mitigate DKIM replay
  - Tolerate modern mail flows that include multi-hop forwarding
  - Tolerate message body modification in particular from mailing lists

Appendix

- Other relevant email authentication drafts
  - draft-kucherawy-dkim-transform
  - draft-kucherawy-dkim-list-canon
  - draft-levine-dkim-conditional
  - draft-vesely-smooth-canon