Poster: Forward Pass: On the Security Implications of Email Forwarding Mechanism and Policy

Enze Liu
UC San Diego
e7liu@ucsd.edu

Gautam Akiwate
Stanford University
gakiwate@cs.stanford.edu

Mattijs Jonker
University of Twente
m.jonker@utwente.nl

Ariana Mirian
UC San Diego
amirian@cs.ucsd.edu

Grant Ho
UC San Diego
grho@eng.ucsd.edu

Geoffrey M. Voelker
UC San Diego
voelker@cs.ucsd.edu

Stefan Savage
UC San Diego
savage@cs.ucsd.edu

Abstract

The critical role played by email has led to a range of extension protocols (e.g., SPF, DKIM, DMARC) designed to protect against the spoofing of email sender domains. These protocols are complex as is, but are further complicated by automated email forwarding — used by individual users to manage multiple accounts and by mailing lists to redistribute messages. In this paper, we explore how such email forwarding and its implementations can break the implicit assumptions in widely deployed anti-spoofing protocols. Using large-scale empirical measurements of 20 email forwarding services (16 leading email providers and four popular mailing list services), we identify a range of security issues rooted in forwarding behavior and show how they can be combined to reliably evade existing anti-spoofing controls. We further show how these issues allow attackers to not only deliver spoofed email messages to prominent email providers (e.g., Gmail, Microsoft Outlook, and Zoho), but also reliably spoof email on behalf of tens of thousands of popular domains including sensitive domains used by organizations in government (e.g., state.gov), finance (e.g., transunion.com), law (e.g., perkinscoie.com) and news (e.g., washingtonpost.com) among others.

Paper Link

Our paper is published at the 8th IEEE European Symposium on Security and Privacy (EuroS&P '23) and can be found here: https://arxiv.org/pdf/2302.07287.pdf

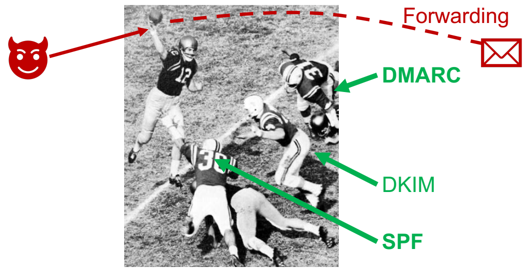
Forward Pass: On the Security Implications of Email Forwarding Mechanism and Policy

Enze "Alex" Liu[1], Gautam Akiwate[2], Mattijs Jonker[3], Ariana Mirian[1],
Grant Ho[1], Geoffrey M. Voelker[1], Stefan Savage[1]

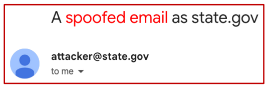
[1] UC San Diego, [2] Stanford University, [3] University of Twente

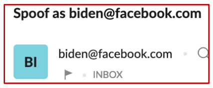
Best Paper Award @ IEEE EuroS&P 23
Finalist @ CSAW Applied Research Competition 23

Summary



- Conduct a large-scale measurement of 20 email forwarding services.
- Identify a range of vulnerable features and practices.
- Uncover attacks that allow an adversary to:
  - Spoof as **~12%** of Alexa top 100k domains such as
  - Or deliver to

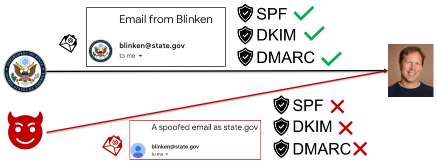

A spoofed email as state.gov
attacker@state.gov
to me


Spoof as biden@facebook.com
BI biden@facebook.com
INBOX

Email Authentication

1

Email had no authentication mechanism when first proposed. Instead, several authentication protocols were added post hoc, namely, SPF, DKIM and DMARC.

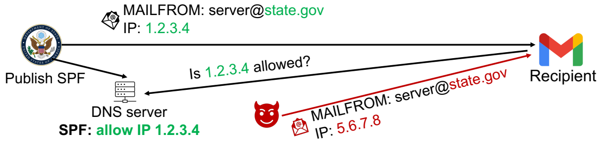

Email from Blinken
blinken@state.gov
to me

A spoofed email as state.gov
blinken@state.gov
to me

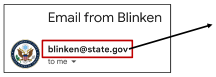
Background: SPF and DMARC

2

SPF: IP-based authentication



DMARC: authenticates the visible header (simplified version)

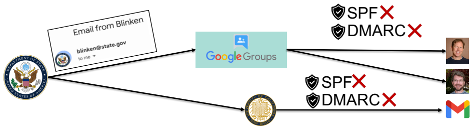

Email from Blinken
blinken@state.gov
to me

- SPF verifies the sending server (server@state.gov)
- Users see the sending user (blinken@state.gov)
- DMARC authenticates the sending user by requiring SPF pass and domain(server) = domain(user)

Forwarding Breaks Authentication

3

Forwarding is used for aggregating email from multiple accounts and massively distribute an email. There exists no standard on how to implement forwarding.


Email from Blinken
blinken@state.gov
to me

Challenge: support forwarding while not breaking authentication

Methodology

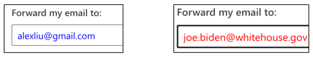
4

- 20 leading forwarding services (16 email providers + four mailing lists).
- Forwarding accounts at all 20 services and receiving accounts at 16 email providers.

Vulnerable Features and Practices

5

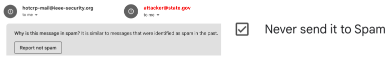
Open forwarding


Forward my email to: alexliu@gmail.com

Forward my email to: joe.biden@whitehouse.gov

Open forwarding allow users to forward to any destination email address, without any verification from the destination address.

Whitelisting


hotcrp-mail@ieee-security.org
to me

attacker@state.gov
to me

Why is this message in spam? It is similar to messages that were identified as spam in the past.

Report not spam

☑ Never send it to Spam

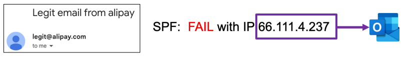
Whitelisting allows a user to overwrite authentication results.

Shared SPF

SPF: allow outlook.com

Domains these days allow the same third-party email provider to send on their behalf.

Relaxed validation


Legit email from alipay
legit@alipay.com
to me

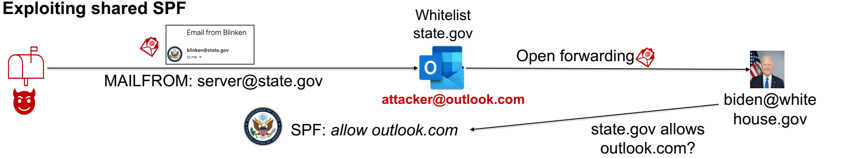
Relaxed validation trusts forwarded email from "high-profile" providers.

Additional vulnerable features and practices:
• Unsolicited DKIM Signature • Quarantine instead of reject • Faulty ARC [2] implementation

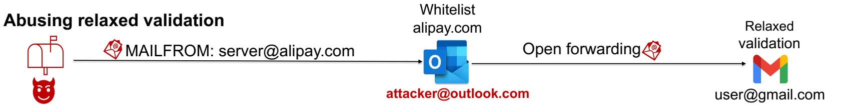
Attacks

6

Exploiting shared SPF


Email from Blinken
blinken@state.gov
to me

Abusing relaxed validation



Additional attacks:
• Leveraging faulty ARC implementation • Laundering spoofed email via mailing lists

Mitigations

7

Short-term mitigations:
• Disable open forwarding • Remove relaxed validation • Separate servers for forwarding • New protocols (e.g., ARC)
Long-term mitigations: more principled design

References

[1] Forward pass picture link: https://en.wikipedia.org/wiki/Forward_pass
[2] Authenticated Received Chain (ARC): RFC 8617