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

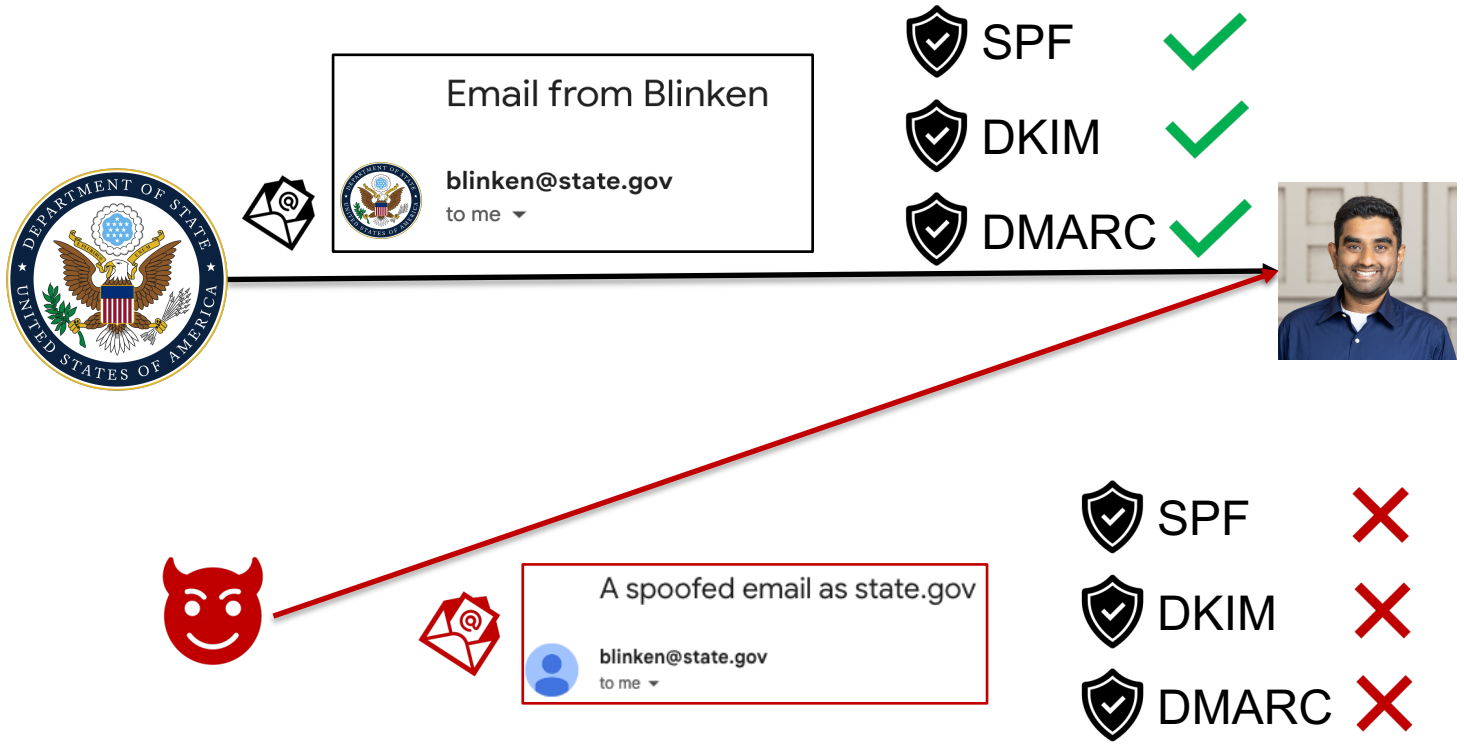
Enze “Alex” Liu, Gautam Akiwate, Mattijs Jonker, Ariana Mirian, Grant Ho, Geoffrey M. Voelker, Stefan Savage

UC San Diego

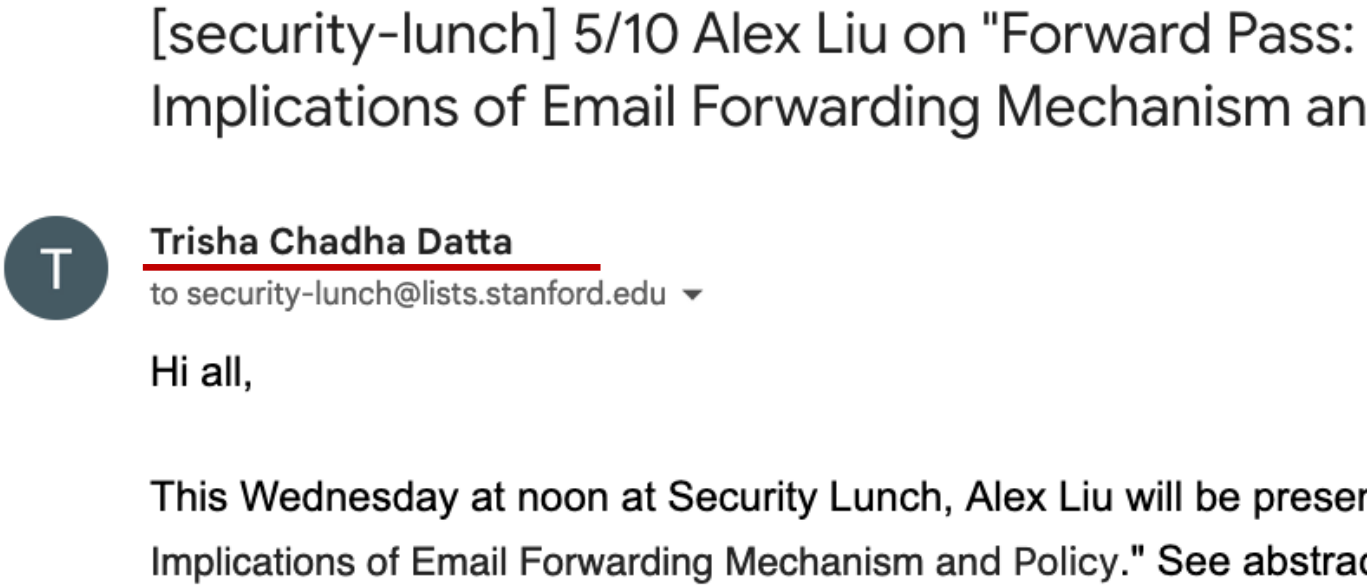
UNIVERSITY OF TWENTE.

https://arxiv.org/abs/2302.07287 *(EuroS&P ‘23)*

Email Authentication in the Simplest Form



Challenges in Email Authentication


[security-lunch] 5/10 Alex Liu on "Forward Pass: Implications of Email Forwarding Mechanism an

T

Trisha Chadha Datta

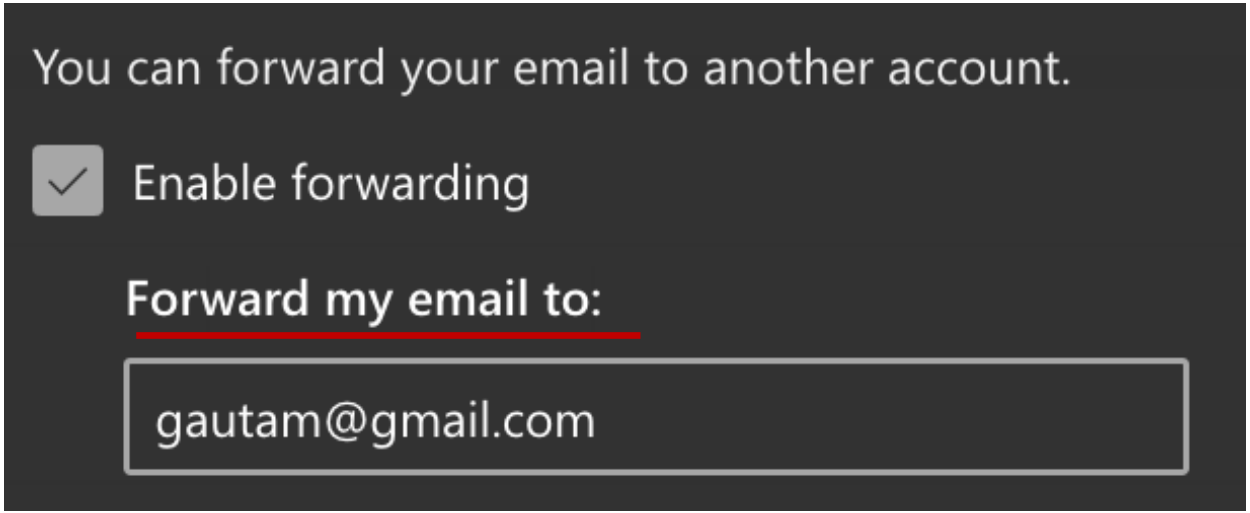
to security-lunch@lists.stanford.edu

Hi all,

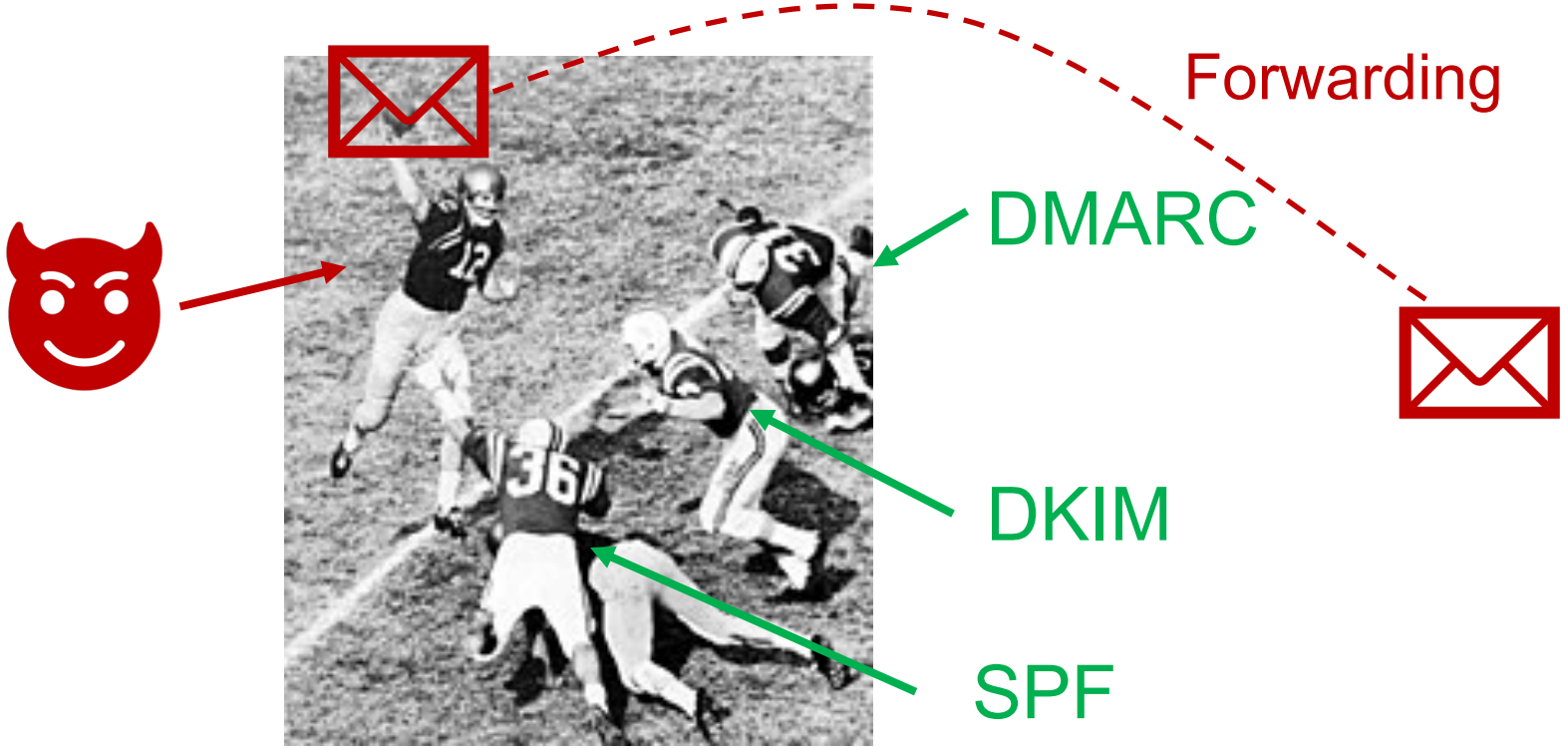
This Wednesday at noon at Security Lunch, Alex Liu will be preser

Implications of Email Forwarding Mechanism and Policy." See abstrac

Challenges in Email Authentication



Forward Pass: A 10,000-foot View



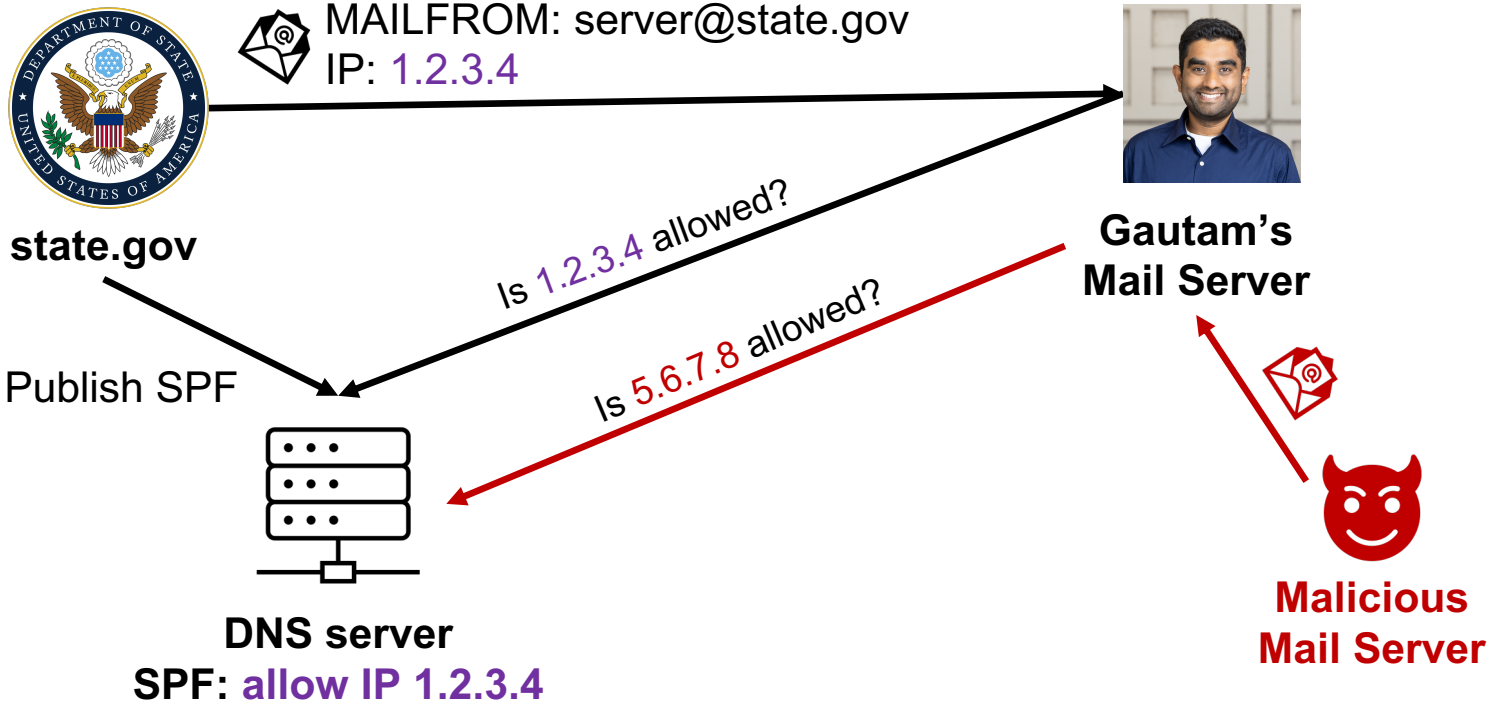
Credit: https://en.wikipedia.org/wiki/Forward_pass

Forward Pass: Contributions

- Goal: forwarding practices and their security implications
- Methodology: 20 services that support forwarding
- Results:
  - A range of assumptions and practices
  - Four distinct kinds of evasion attacks

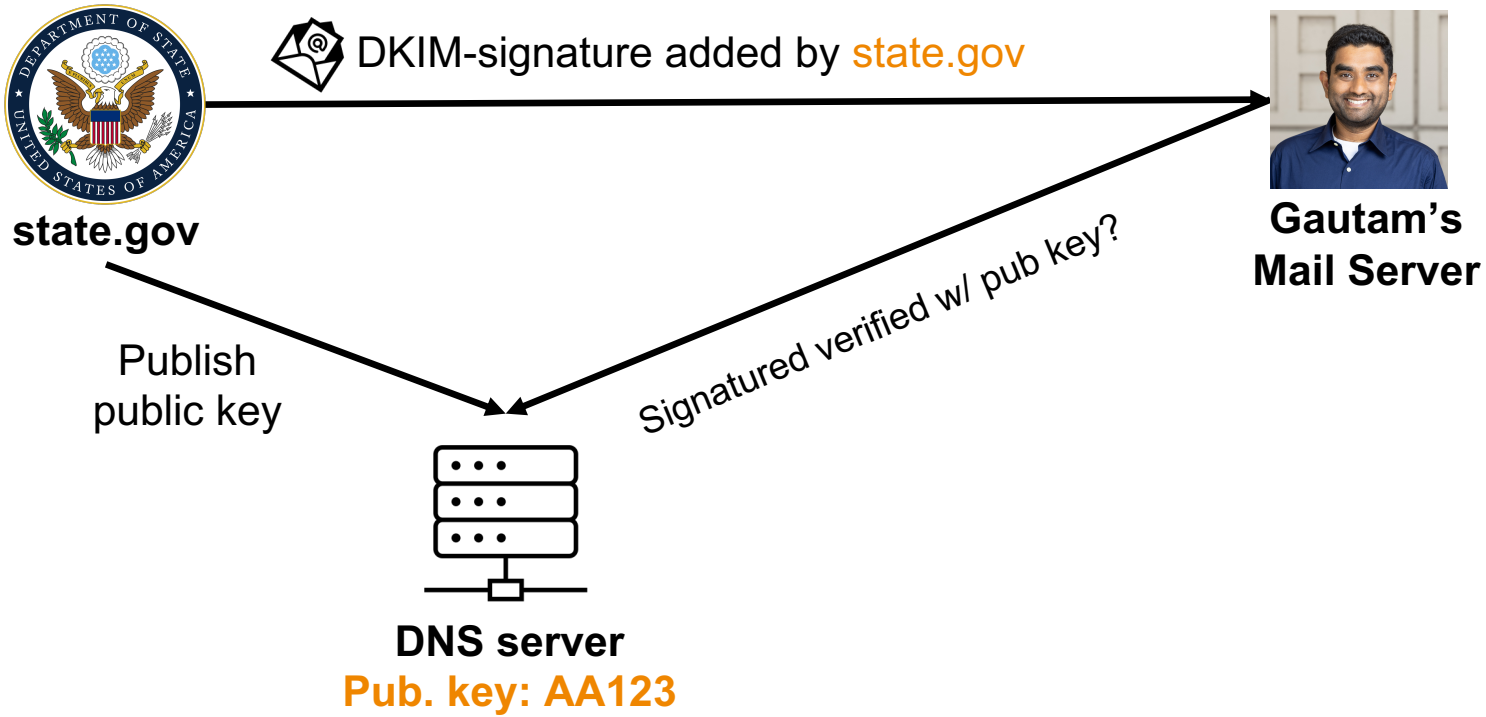
Background: SPF

IP-based authentication



Background: DKIM

Signature-based authentication

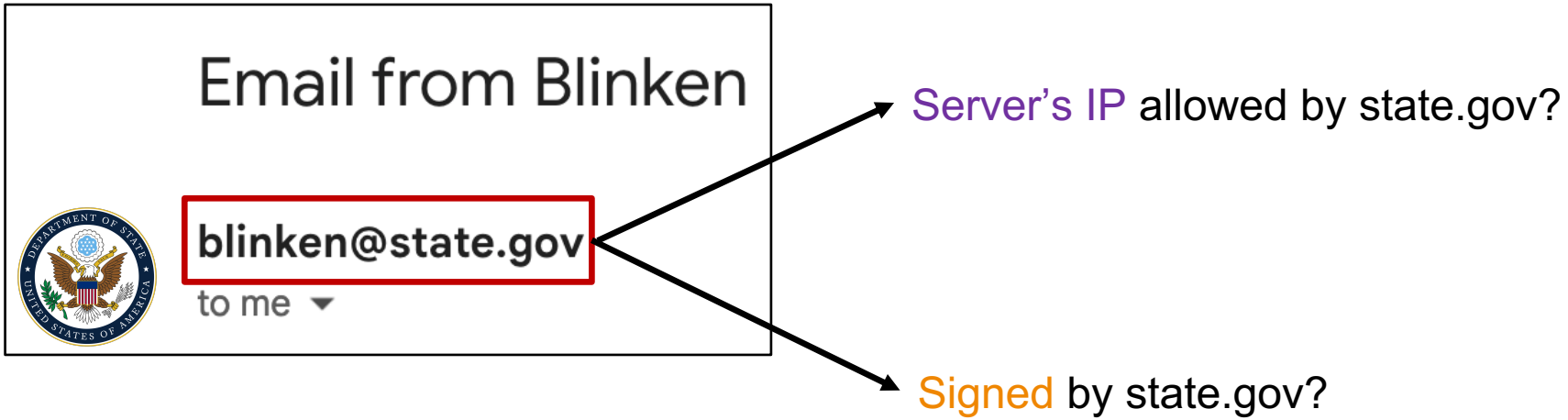


Background: DMARC

- FROM header is not authenticated

- Combines SPF and DKIM to authenticate FROM
  - If SPF passes, check if Domain(MAILFROM) = Domain(FROM)
  - If DKIM passes, check if Domain(DKIM-Sign) = Domain(FROM)

Authenticating an Email from state.gov



Methodology

- Goal: forwarding practices and their security implications
- 16 mail providers + 4 mailing lists

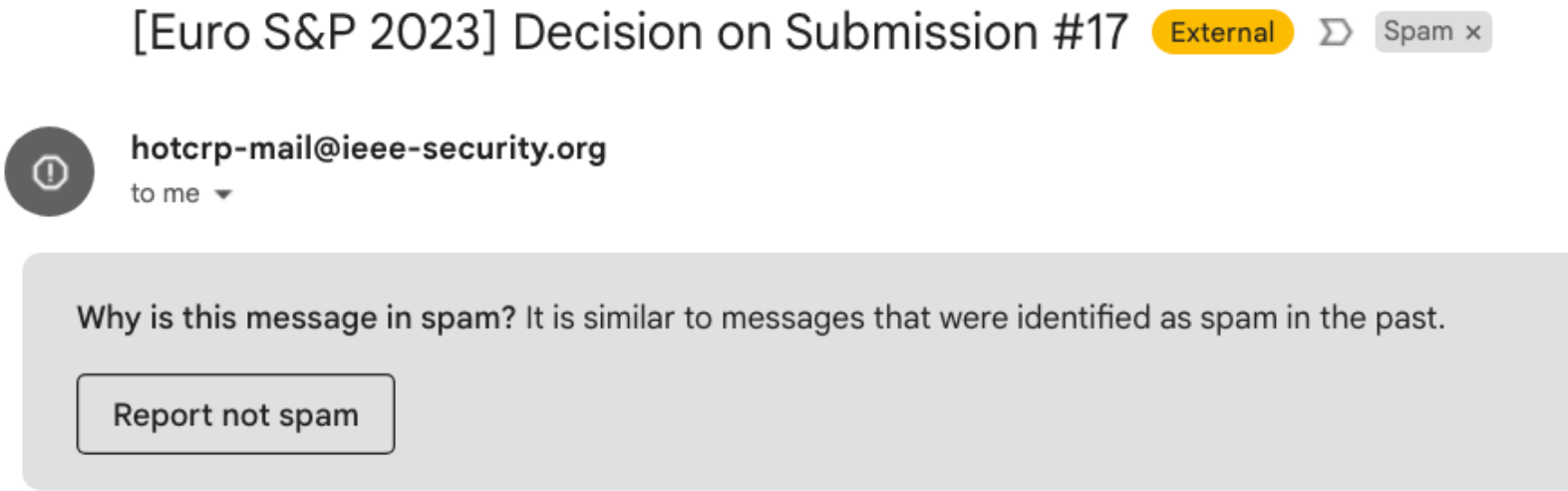
Practices

Assumptions

Attacks

https://arxiv.org/abs/2302.07287

Practice: Whitelisting

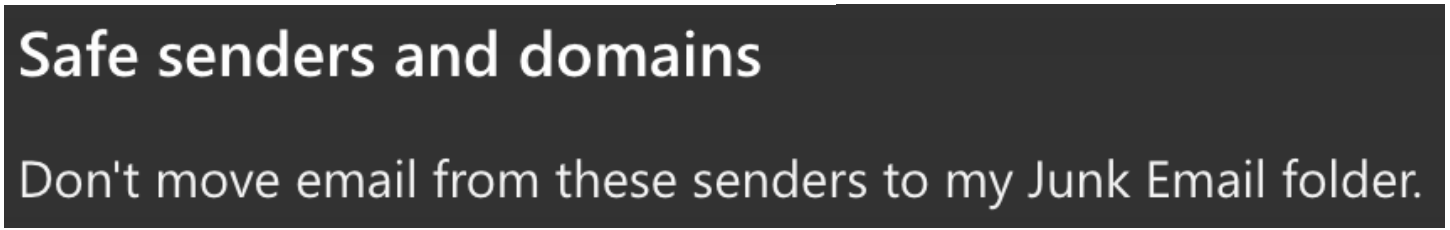


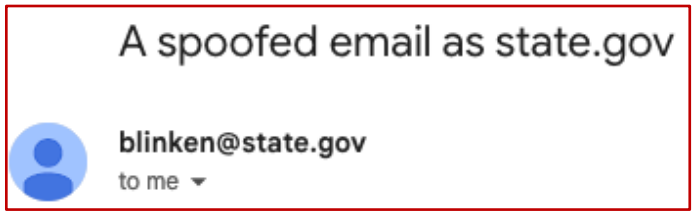
https://arxiv.org/abs/2302.07287

Practice: Whitelisting

Gmail: ☑ Never send it to Spam

Outlook:

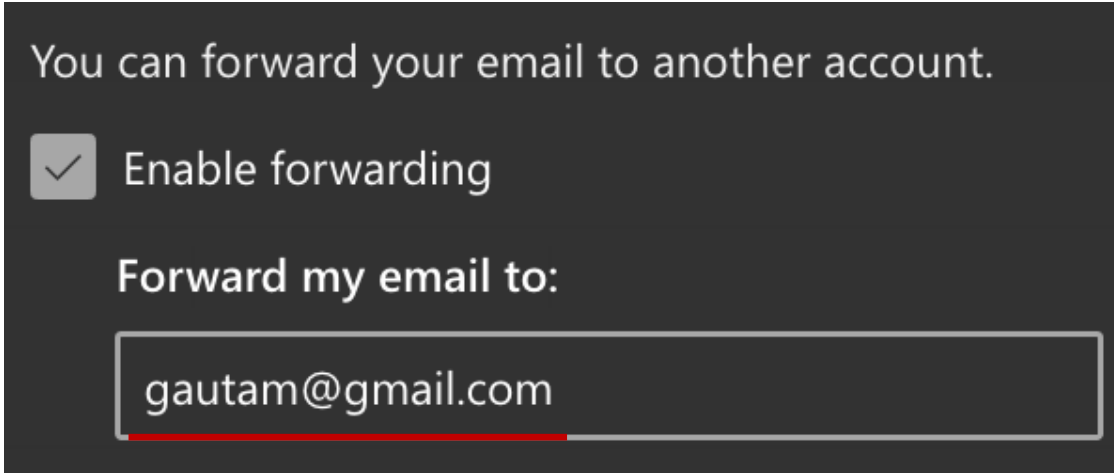




Whitelisting allows a malicious user to bypass authentication checks for spoofed emails

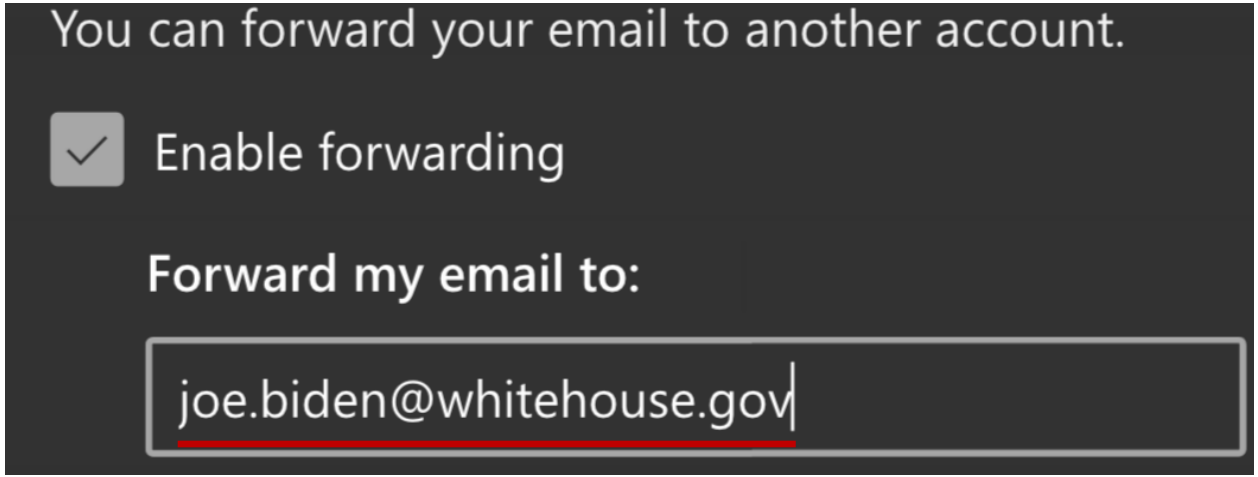
https://arxiv.org/abs/2302.07287

Practice: Open Forwarding



https://arxiv.org/abs/2302.07287

Practice: Open Forwarding

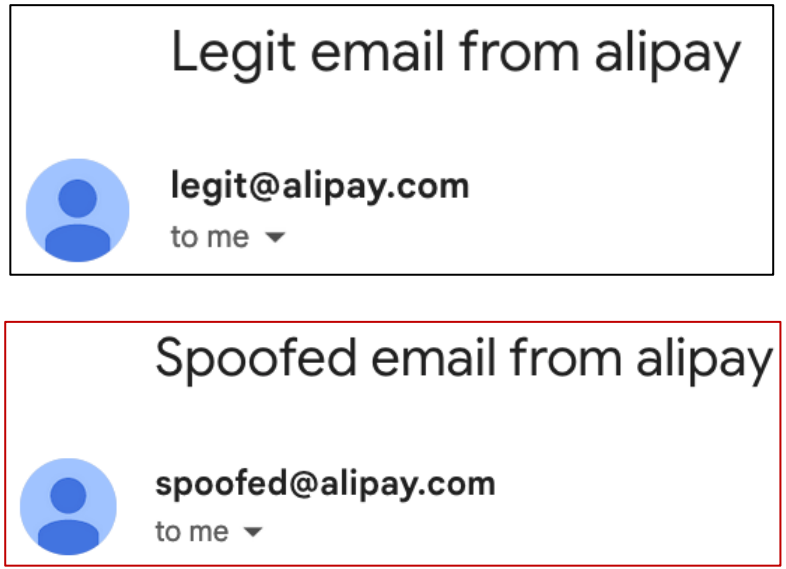


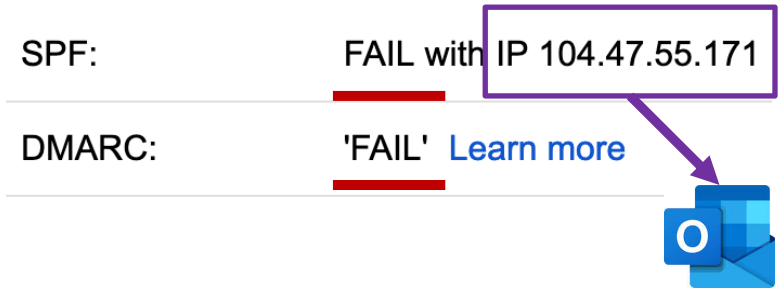
Open forwarding allows a malicious user to forward to arbitrary destination without authorization

https://arxiv.org/abs/2302.07287

Practice: Relaxed Validation

Trusting forwarded email messages from certain providers





Relaxed validation assumes that upstream providers do not forward spoofed emails

https://arxiv.org/abs/2302.07287

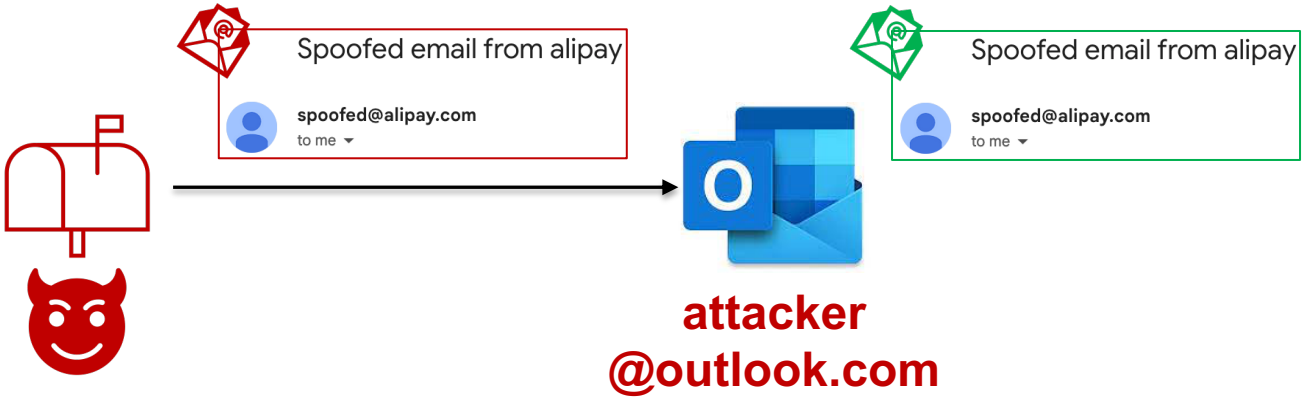
Attack: Relaxed Validation

https://arxiv.org/abs/2302.07287

Attack: Relaxed Validation

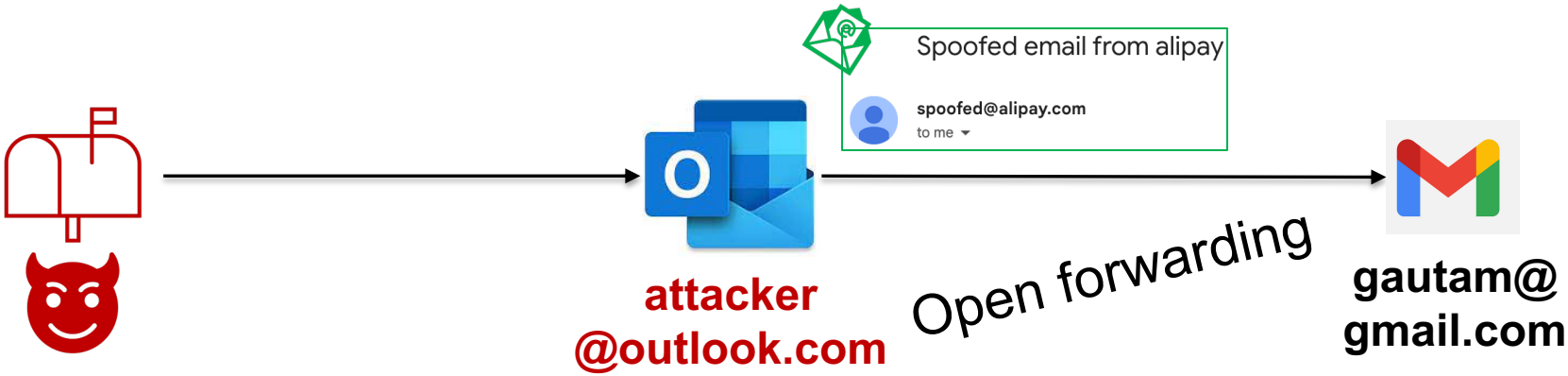
https://arxiv.org/abs/2302.07287

Attack: Relaxed Validation



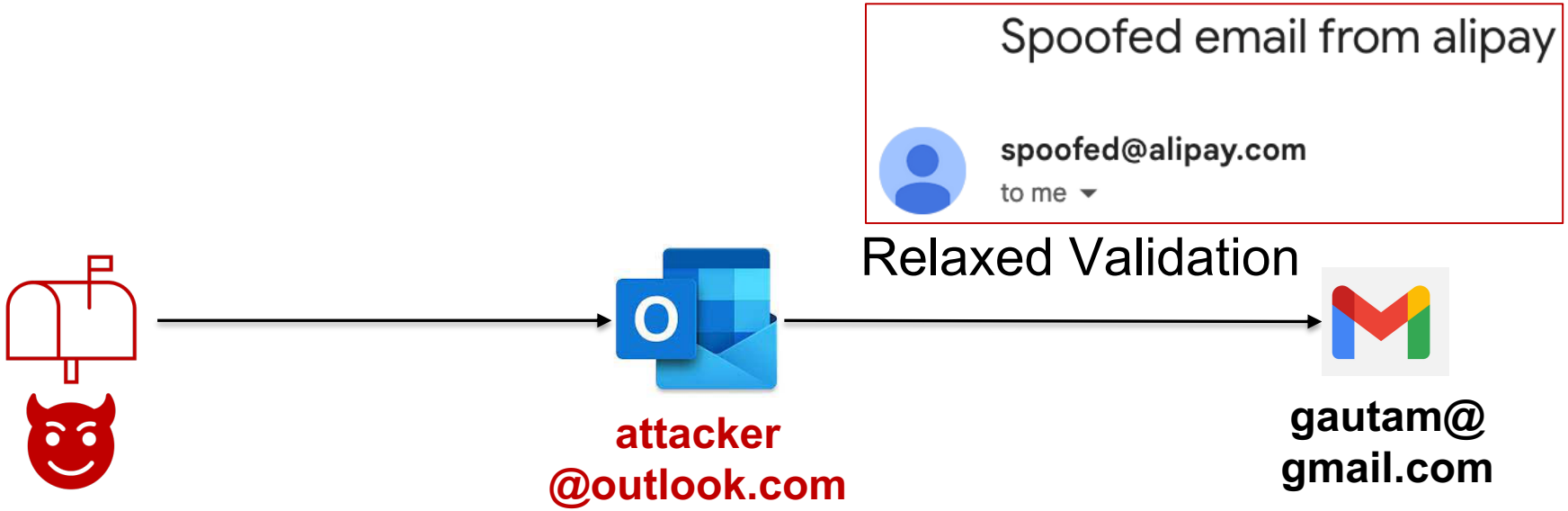
https://arxiv.org/abs/2302.07287

Attack: Relaxed Validation



https://arxiv.org/abs/2302.07287

Attack: Relaxed Validation



https://arxiv.org/abs/2302.07287

SPF's Outdated Assumption

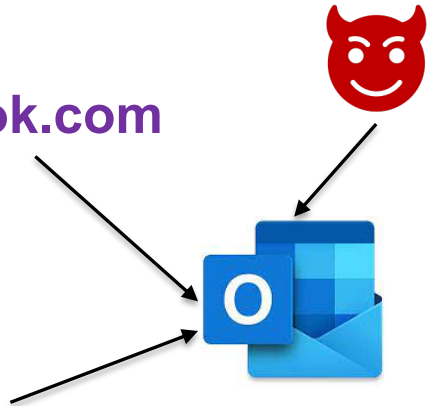
- When SPF was created

SPF: allow 1.2.3.4

SPF: allow 5.6.7.8

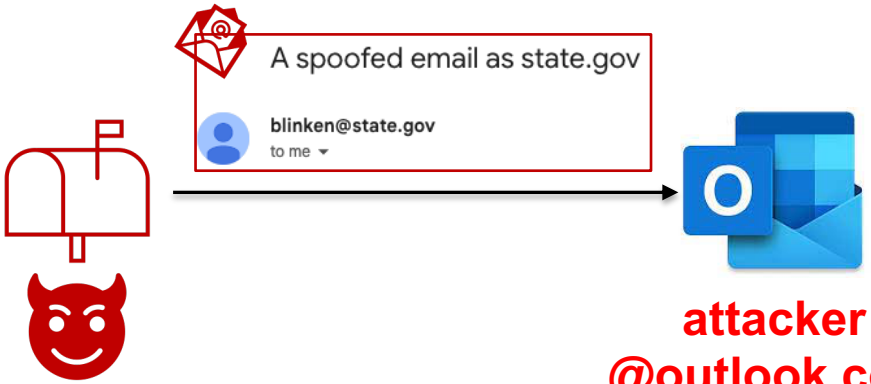
- Nowadays: shared SPF

SPF: allow outlook.com



SPF: allow outlook.com

Attack: Shared SPF



SPF: allow outlook.com

https://arxiv.org/abs/2302.07287

Attack: Shared SPF

SPF: allow outlook.com

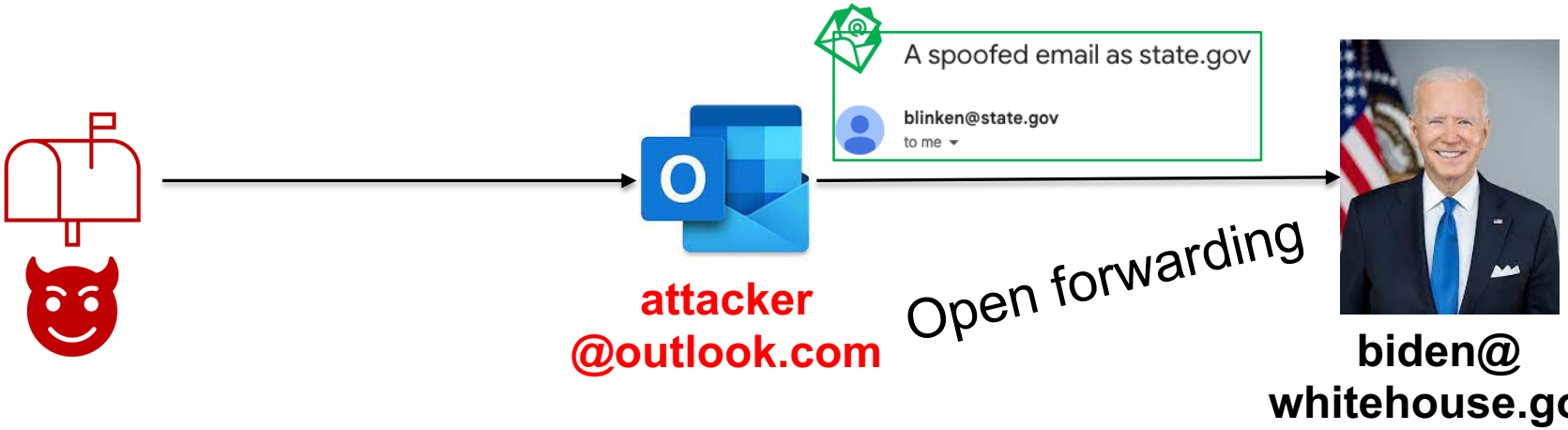
https://arxiv.org/abs/2302.07287

Attack: Shared SPF

SPF: allow outlook.com

https://arxiv.org/abs/2302.07287

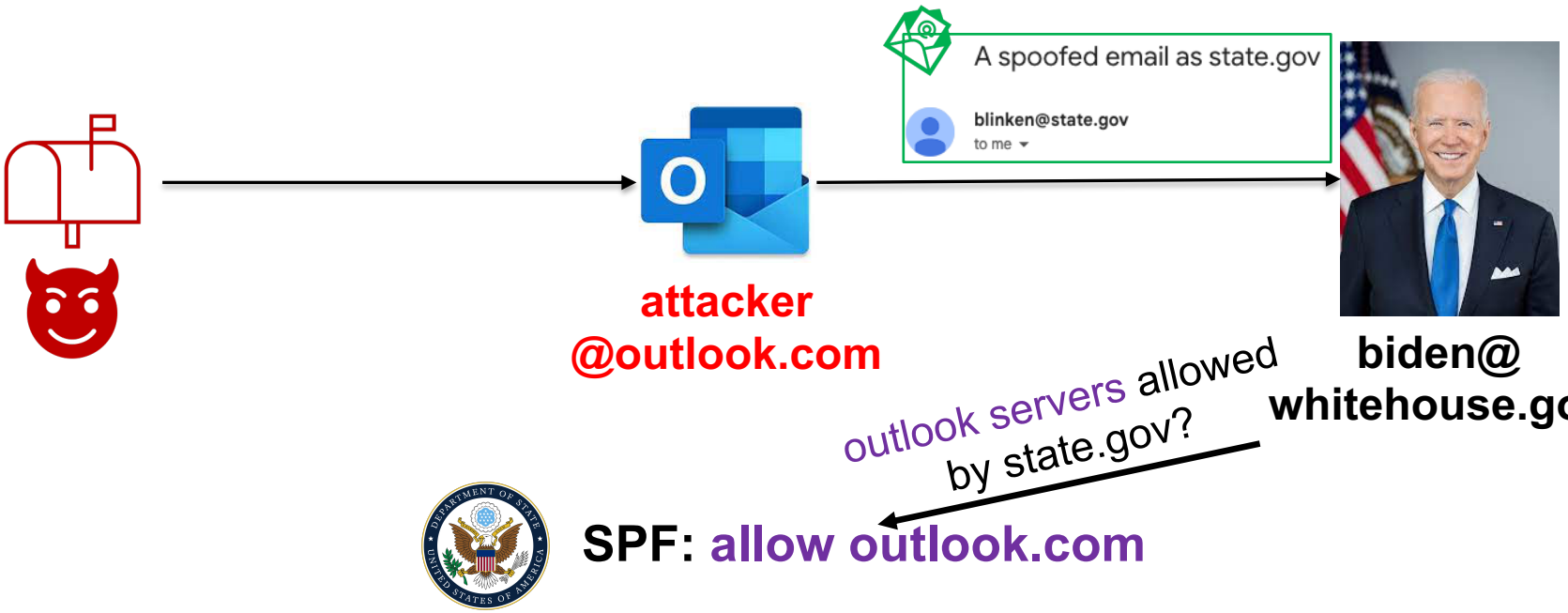
Attack: Shared SPF



SPF: allow outlook.com

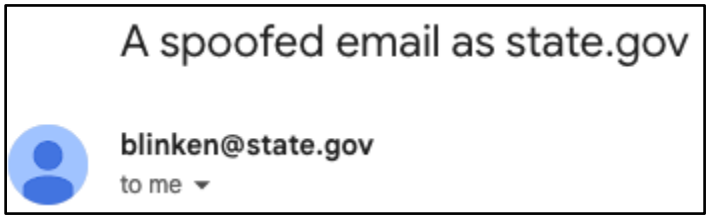
https://arxiv.org/abs/2302.07287

Attack: Shared SPF



https://arxiv.org/abs/2302.07287

Attack: Shared SPF



https://arxiv.org/abs/2302.07287

Root Causes

- Forward works at odds with authentication protocols
- Ad-hoc implementation decisions
- No guidelines on how to implement forwarding
- SPF’s outdated assumption

https://arxiv.org/abs/2302.07287

Mitigations

- Disable open forwarding
- Remove relaxed validation
- Separate servers for sending and forwarding
- New protocols (e.g., ARC)

https://arxiv.org/abs/2302.07287

Disclosure

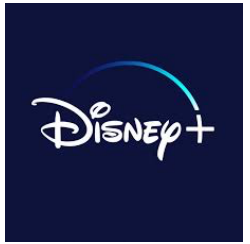
- All providers acknowledged the reported issues

- Some fixed; some partially fixed; some didn’t

https://arxiv.org/abs/2302.07287

Summary

- Goal: forwarding practices and their security implications
- Large-scale measurement of 20 forwarding services
- Forwarding practices, assumptions, and attacks



https://arxiv.org/abs/2302.07287

If You Can Only Remember One Thing

e7liu@eng.ucsd.edu

e7liu.github.io

https://arxiv.org/abs/2302.07287