

# 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>

