Paper: https://bit.ly/www-bypass

Unfiltered: Measuring Cloud-based Email Filtering Bypasses

Sumanth Rao[1] Enze "Alex" Liu[1] Grant Ho[2] Geoffrey M. Voelker[1] Stefan Savage[1]

[1]UC San Diego [2]UChicago

1. Summary

- Third-party **email filtering services** (e.g, Proofpoint) scan inbound email for threats and deliver *safe* email to the **email hosting provider** (e.g,Gmail , Exchange Online)
- **Challenge:** Email filtering services can be **bypassed** if the email hosting provider is not configured to ***only*** accept messages that arrive from the email filtering service.
- **Using an empirical measurement of *edu* and *com* domains, we show that 80% of popular domains using cloud-based email filtering services can be bypassed in this manner**

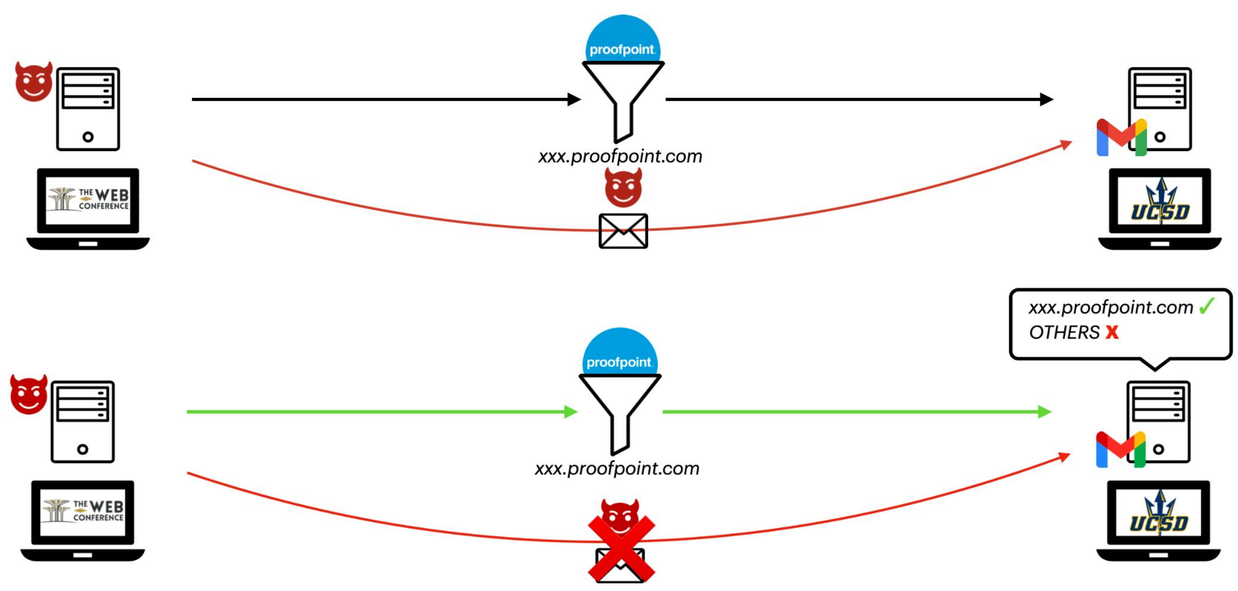

Fig 2: Incorrect and correct configuration for filtering inbound email

3. Inferring Bypass

- Infer if the domain's email provider *only* accepts mail from filtering service and **rejects** other attempts
- Initiate an SMTP transaction with the mail provider and attempt to send email to a *valid address*
  - *NOT rejected* → Vulnerable to bypass
  - Gmail and Zoho → Reject at *RCPT* stage (before sending)
  - Exchange → Reject at *DATA* stage (after sending)
- Valid addresses → Use "role" accounts (e.g, *postmaster@domain*) to avoid undue spam (e.g, Exchange)

Filtering Serv.	Exchange	Gmail	Total
Proofpoint	415/541 (77%)	152/175 (87%)	567/716 (79%)
Barracuda	186/244 (76%)	26/27 (96%)	212/271 (79%)
Mimecast	113/171 (66%)	69/73 (95%)	182/244 (75%)
Cisco	124/139 (89%)	15/18 (83%)	139/157 (89%)
TrendMicro	30/30 (100%)	10/12 (83%)	40/42 (95%)
Sophos	16/18 (89%)	7/9 (78%)	23/27 (85%)
Cloudflare	8/8 (100%)	10/14 (71%)	18/22 (82%)
Trellix	9/13 (69%)	5/7 (71%)	14/20 (70%)
AppRiver	13/13 (100%)	6/6 (100%)	19/19 (100%)
ForcePoint	11/13 (85%)	1/1 (100%)	12/14 (86%)
Fortinet	13/14 (93%)	1/1 (100%)	14/15 (93%)
Broadcom	10/12 (83%)	3/3 (100%)	13/15 (87%)
HornetSecurity	2/8 (25%)	1/1 (100%)	3/9 (33%)
N-able	3/3 (100%)	–	3/3 (100%)
Spamhero	2/2 (100%)	1/1 (100%)	3/3 (100%)
Total	955/1,229 (78%)	307/348 (88%)	1,262/1,577 (80%)

Tab 1: Inferring domain bypassability for top 15 filtering services across top 2 hosting providers (4 Zoho domains were all misconfigured)

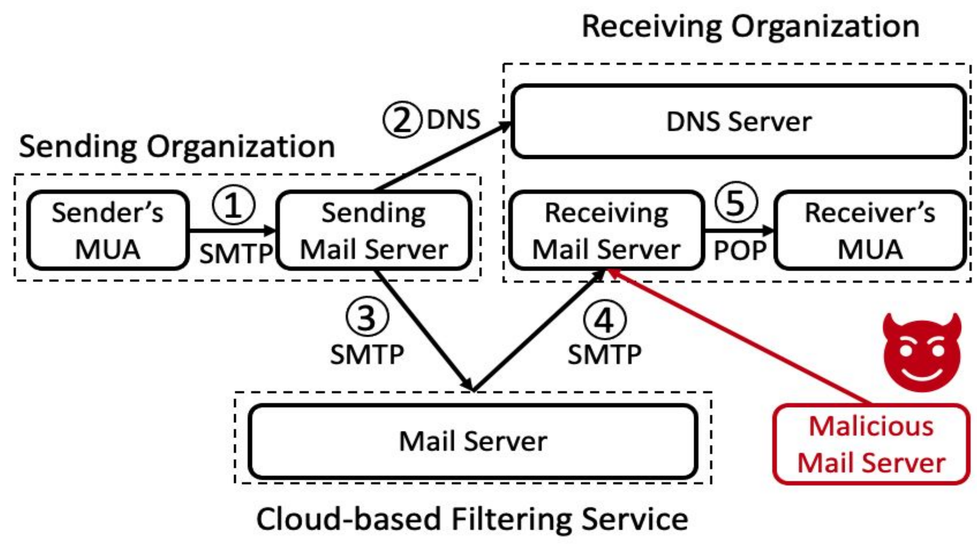

Fig 1: Steps to bypass email filtering services

2. Methodology

- Tested a corpus of **889 *edu*** domains and **1,429 *com*** domains using:
  - **15** leading cloud-based email filtering services
  - **3** popular email hosting providers (, , Zoho)
- **Map** each domain to their filtering service and email hosting provider
- **Probe** the integrity of the binding b/w the filtering service and email hosting provider
- **Validate** the possibility of bypass (e.g, via manual contacts, automated bounces)

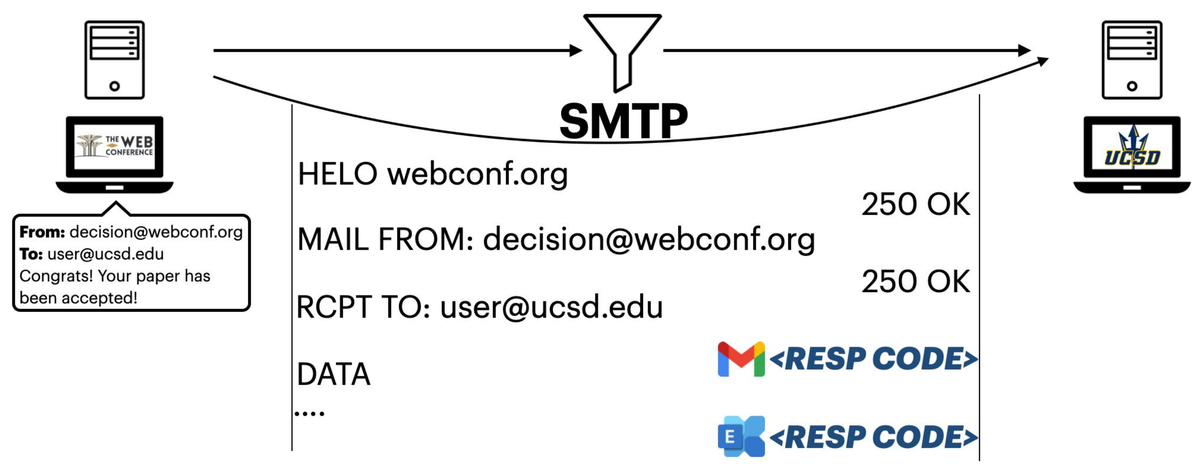

Fig 3: Inferring bypass for Exchange and Gmail using error codes from SMTP interactions.

4. Mapping Email Filter/Provider

- Mapped domains to filtering service using MX and banner info (Step 2/3, Fig 1)
- Inferred email hosting provider using externally testable data:
  - Gmail and Zoho → pre-created accounts (e.g, *postmaster@domain*)
  - Exchange → Unique DNS record exists per domain
- To test if the email hosting is in active use?
  - Additional filtering using Sender Policy Framework (SPF)

5. Results & Disclosure

- **80%** of domains in our data are misconfigured overall, with Gmail misconfigured more (88%) than Exchange (78%)
- Report potential misconfiguration reasons (e.g., missing/unclear documentation, concerns of deliverability)
- **Disclosed** to filtering service providers and worked with them to notify customers/domains and improve setup documentation