Email Spoofing with SMTP Smuggling:

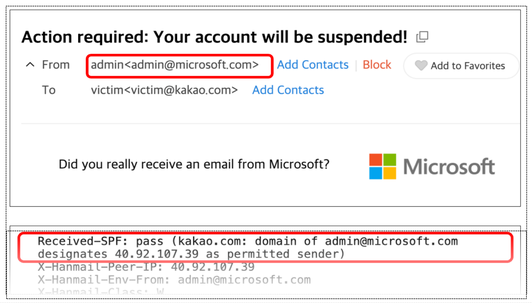
How the Shared Email Infrastructures Magnify this Vulnerability

Chuhan Wang, Chenkai Wang, Songyi Yang, Sophia Liu, Jianjun Chen, Haixin Duan, Gang Wang

Southeast University, Tsinghua University, University of Illinois Urbana-Champaign

Why should you care?

- SMTP smuggling is a technique allowing attackers to **spoof email addresses without authentication**. Name a few threats:
  - Same-domain addresses
    - Student impersonate professor
    - Intern impersonate CEO
  - Cross-domain addresses
    - Gmail user impersonate Google
    - Outlook user impersonate Microsoft



PoC: Attacker impersonates admin@microsoft.com

Our work

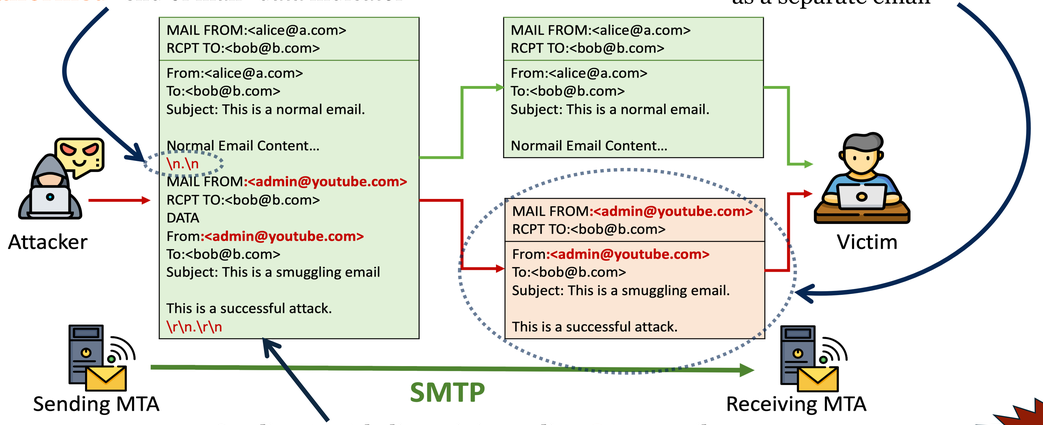
- A **comprehensive** measurement of SMTP smuggling across wide range of targets: **public and private** email services, open-source email software, commercial email gateways.
- New measurement methodologies enabling **automatic and non-intrusive** vulnerability test and advisory **at scale!**
- Reveals real-world vulnerable services and software and insights of how shared SMTP infrastructure magnifies the impact.

Measurement results

- **19 of 22** public email services were vulnerable.
- **23 of 48** university email services were vulnerable. (via user study)
- **1,577** of Tranco top-10,000 domains were vulnerable. (via non-intrusive test)
- **5 of 5** open-source email software were vulnerable.
- **1 of 2** email gateways was vulnerable.

How SMTP smuggling works?

1. Attacker assemble the smuggled email with a **malformed** "end of mail" data indicator

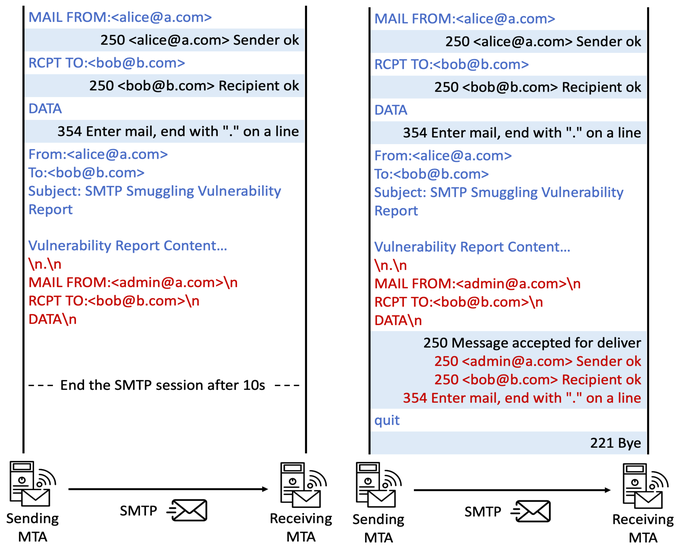


2. Sending MTA believes it is sending **ONE** email

3. Vulnerable receiving MTA processes the smuggled portion as a separate email

How we non-intrusively measure private services at scale

- We look to cover more private email services, but...
  1. Many would be impossible for us to get inbox access;
  2. We need automation.
- We develop the non-intrusive method as follows:
  1. We send the test payload with a delay after sending the malformed indicator;
  2. If receiving end replies, it is vulnerable. We then send our vulnerability disclosure message;
  3. If not, it is not vulnerable, and we terminate the connection so no full emails will enter inbox.
- To verify its accuracy, we use both user study and a DNS side-channel of DKIM signature in test payload.



Vulnerable receiving MTA replies prematurely (Right)

Shared email infrastructures magnifies the impact

- Modern email systems employ DMARC, which uses SPF **or** DKIM to verify email senders.
- SPF checks the sender's IP address.
- Attackers with access to any account of a shared email infrastructure can spoof any other hosted domains.

Email Service	Shared SPF Domains
outlook.com	**81,718**
gmail.com	**63,225**
yandex.ru	4,838
zoho.com	4,074
qq.com	1,713
mail.ru	999
fastmail.com	768
daum.net	87
yahoo.com	62
icloud.com	47

Email services shared by multiple domains

Responsibly Disclosed!

Insights

- **The centralization of email services magnified SMTP smuggling attacks.**
- Attackers could spoof well-known domains by exploiting SMTP smuggling and the shared SPF infrastructure.

Full Paper

https://nw.ci/smuggle