34TH USENIX SECURITY SYMPOSIUM

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

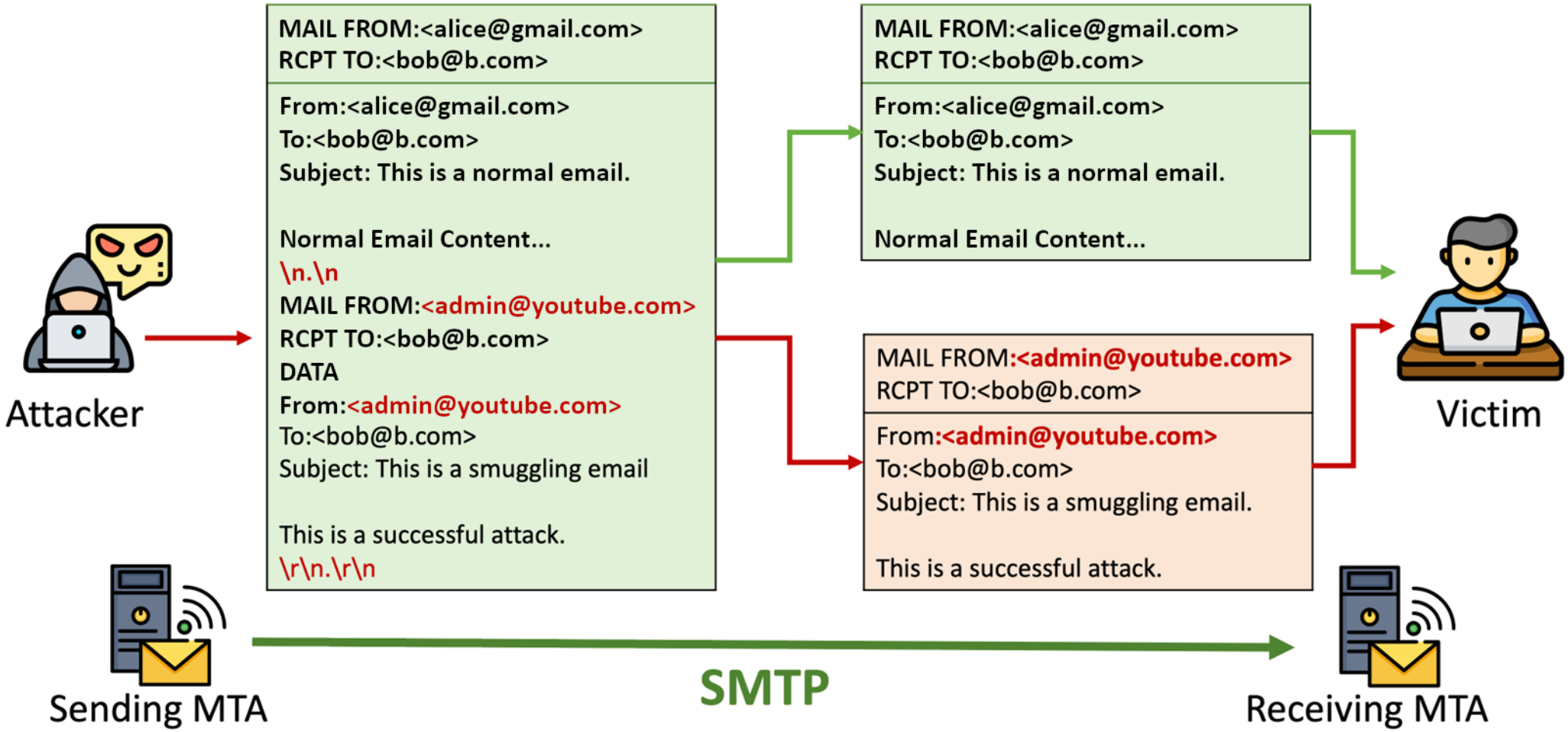
東南大學
SOUTHEAST UNIVERSITY

清華大學
Tsinghua University

UNIVERSITY OF ILLINOIS
URBANA-CHAMPAIGN

What is SMTP Smuggling?

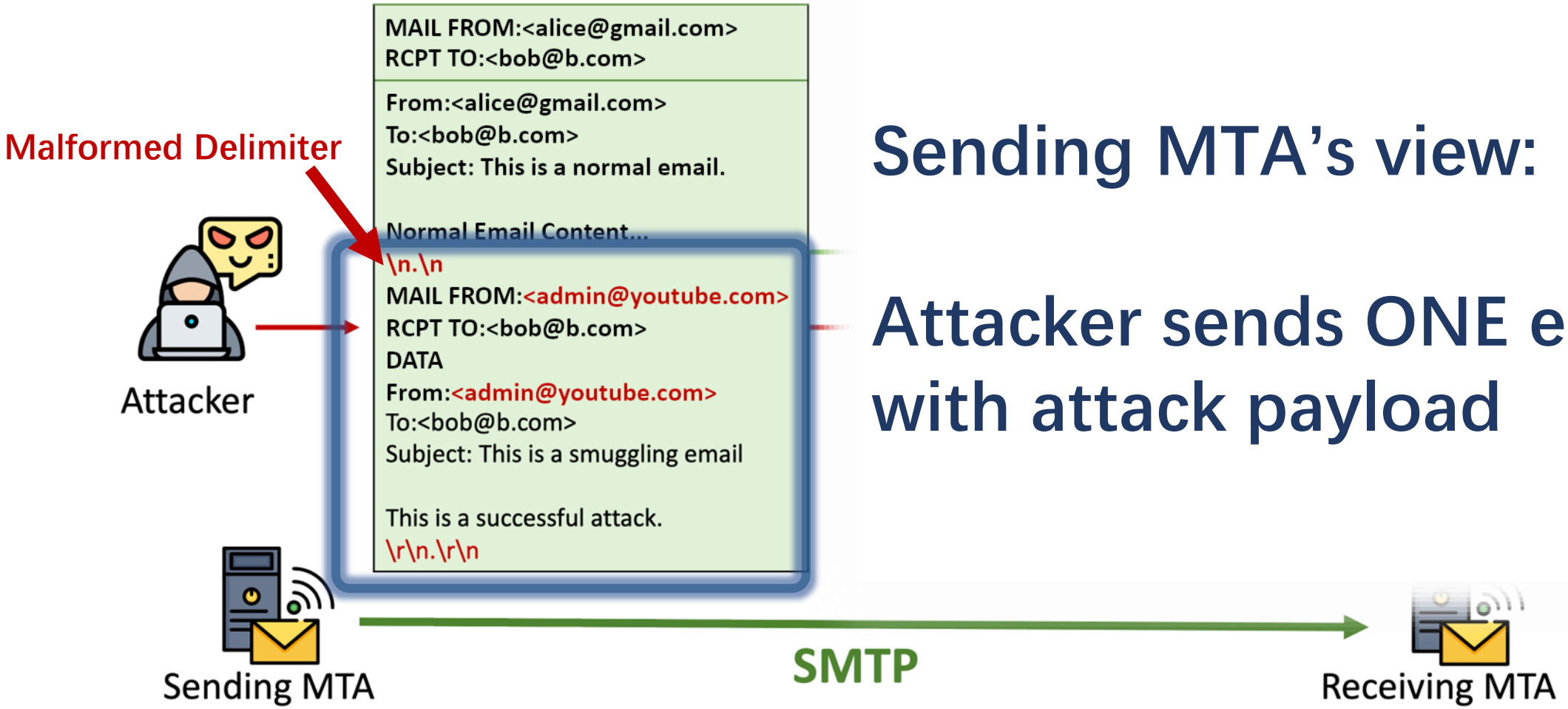
- **SMTP Smuggling:** *a new kind of email spoofing attack[1] which can bypass the protection of SPF and DMARC.*



[1] https://sec-consult.com/blog/detail/smtp-smuggling-spoofing-e-mails-worldwide/

What is SMTP Smuggling?

- **SMTP Smuggling:** *a new kind of email spoofing attack[1] which can bypass the protection of SPF and DMARC.*



Sending MTA's view:

Attacker sends ONE email with attack payload

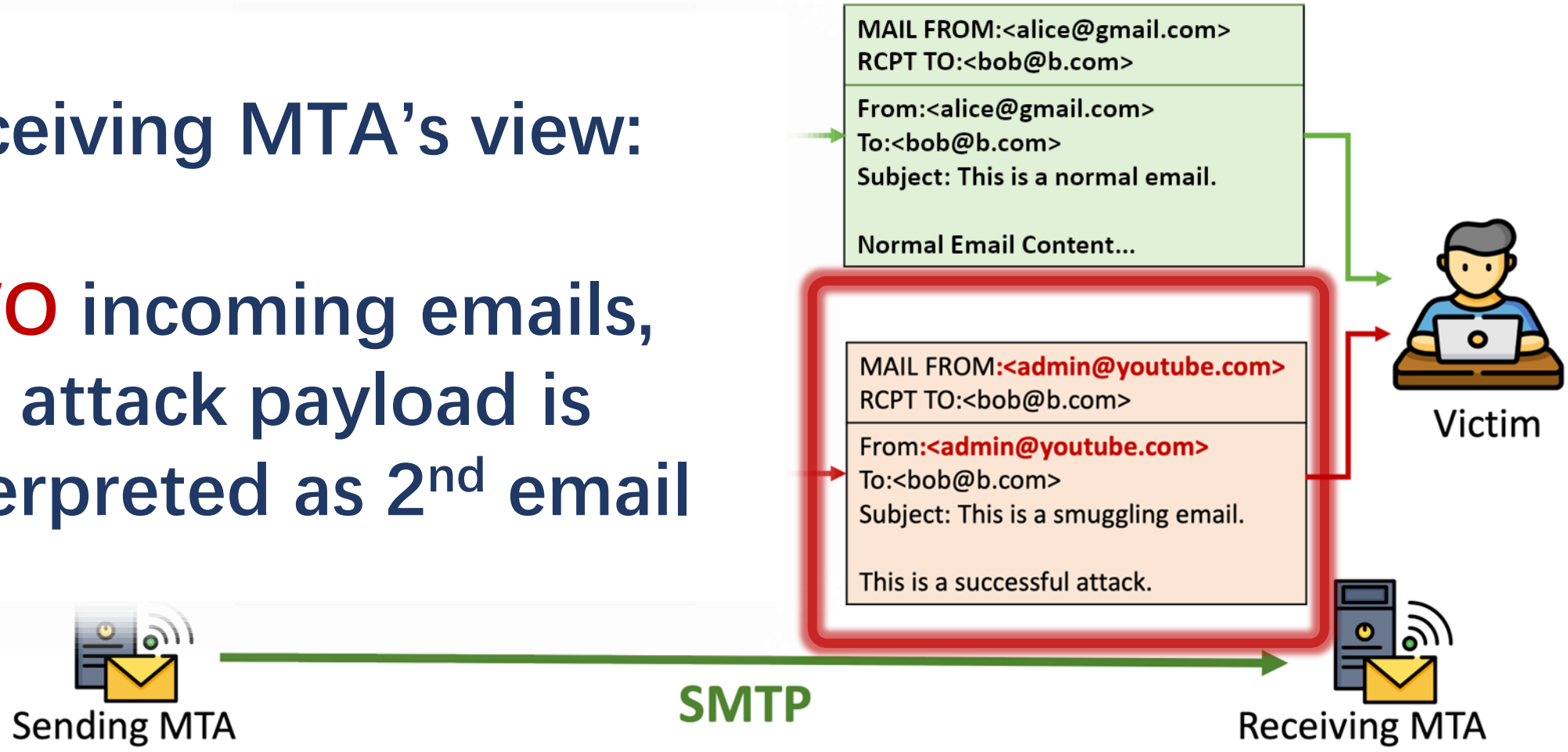
[1] https://sec-consult.com/blog/detail/smtp-smuggling-spoofing-e-mails-worldwide/

What is SMTP Smuggling?

- **SMTP Smuggling:** *a new kind of email spoofing attack[1] which can bypass the protection of SPF and DMARC.*

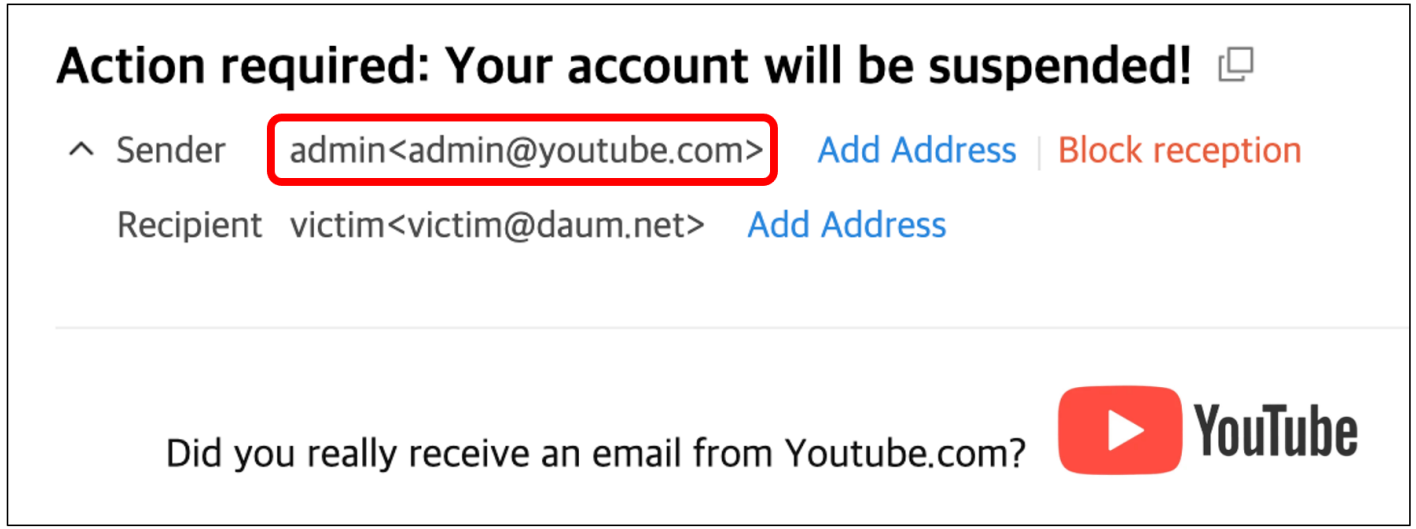
Receiving MTA's view:

TWO incoming emails, the attack payload is interpreted as 2nd email



[1] https://sec-consult.com/blog/detail/smtp-smuggling-spoofing-e-mails-worldwide/

Why is This a Serious Threat?




```
Received-SPF: pass (mx.daum.net: domain of admin@youtube.com designates
209.85.215.176 as permitted sender)
X-Hanmail-Peer-IP: 209.85.215.176
X-Hanmail-Env-From: admin@youtube.com
X-Hanmail-Class: W
X-Kakaomail-MID: Cj38cQAAHJ0AAAGRJ/A5HAAZAl4=
X-Hermes-Message-Id: s76MjeNA01816319049
Message-Id: <202408062245.s76MjeNA01816319049@dmail-rmail-pgvm45>
From: admin@youtube.com
To: victim@daum.net
Subject: Action required: Your account will be suspended!
Date: Tue, 06 Aug 2024 21:45:35 -0000
```

Attacker use **free Gmail account** to spoof ***admin@youtube.com*** to any user of daum.net.

YouTube Gmail

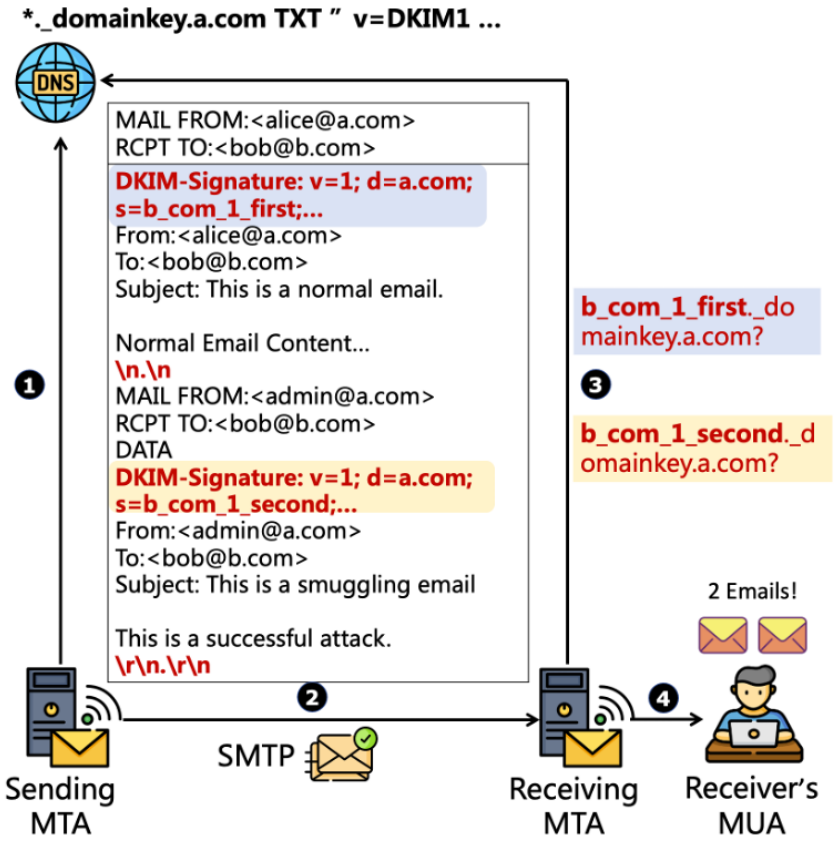
Shares same SPF Infrastructure

Victim receiving "smuggled" YouTube emails from Gmail

Gmail's sending IP passes SPF for youtube.com

Our Research

- **Goal:** *Conduct a comprehensive measurement of SMTP smuggling over a wide range of email infrastructures.*
- **Targets**
  - Public email services
  - Private email services
  - Open-source email software
  - Email gateways
- **Methodology: test *private* email services at scale**
  - User study
  - **DKIM verification side-channel:** monitor DNS queries for DKIM signature in attack payload
  - **Non-intrusive test method:** only delivers a report if vulnerable



DKIM verification side-channel

Results

- **Research Findings**
  - Public email services
    - **19 of 22** public email services were vulnerable.
  - Private email services
    - **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)
  - Open-source email software
    - **5 of 5** open-source email software were vulnerable.
  - Email gateways
    - **1 of 2** email gateways was vulnerable.

Research Findings

- **Shared SPF Infrastructures amplifies cross-domain SMTP smuggling attacks**

Outlook		Gmail	
Rank	**Domain**	**Rank**	**Domain**
3	microsoft.com	1	google.com
15	instagram.com	8	youtube.com
19	live.com	13	twitter.com
28	bing.com	14	cloudflare.com
31	microsoftonline.com	36	fastly.net
44	github.com	37	netflix.com
46	sharepoint.com	38	googlesyndication.com
53	skype.com	41	googleusercontent.com
56	digicert.com	43	youtu.be
61	msn.com	48	pinterest.com

Top 10 Domains within Shared SPF Infrastructure of Outlook and Gmail

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

Shared SPF Infrastructure for Public Email Services

Research Findings

- **Use of common email infrastructures (gateway services and software) has contributed to the propagation of SMTP smuggling attacks.**

Rank	Domain	Infrastructure
5	amazonaws.com	Amazon
10	akamai.net	Proofpoint
12	akamaiedge.net	Proofpoint
14	cloudflare.com	Postfix
15	instagram.com	Proofpoint
25	akadns.net	Proofpoint
27	amazon.com	Amazon
30	wikipedia.org	Postfix
39	wordpress.org	Postfix
67	yandex.net	Yandex

Top 10 Domains Influenced by SMTP Smuggling (Identified by Non-Intrusive Tests)

Infrastructure	Type	Vulnerable Domain
Proofpoint	Gateway	512
Postfix	Software	316
Cisco	Gateway	77
Yandex	Service	70
Sendmail	Software	36
Exim	Software	32
Amazon	Service	29
Bytedance	Service	10
Netease	Service	8
Forcepoint	Gateway	7

Top 10 Vulnerable Email Infrastructures

Thanks!

Full Paper

https://nw.ci/smuggle

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

SOUTHEAST UNIVERSITY

Tsinghua University

UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN