usenix
THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

FakeBehalf: Imperceptible Email Spoofing Attacks against the Delegation Mechanism in Email Systems

Jinrui Ma[1], Lutong Chen[1], Kaiping Xue[1], Bo Luo[2], Xuanbo Huang[1], Mingrui Ai[1], Huanjie Zhang[1], David S.L. Wei[3], Yan Zhuang[1]

[1] University of Science and Technology of China

[2] The University of Kansas

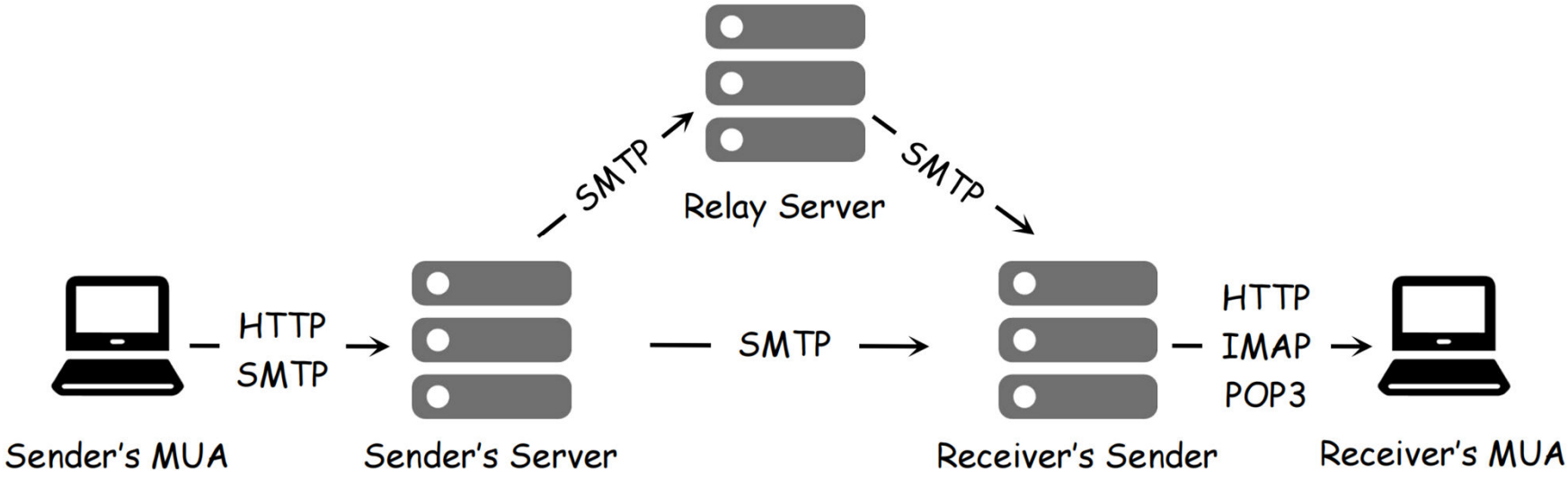
[3] Fordham University

Outline

- **Background**
- Attack model
- Security Issues within Email Delegation
- Results
- Defensive measures

Background: Email transmission

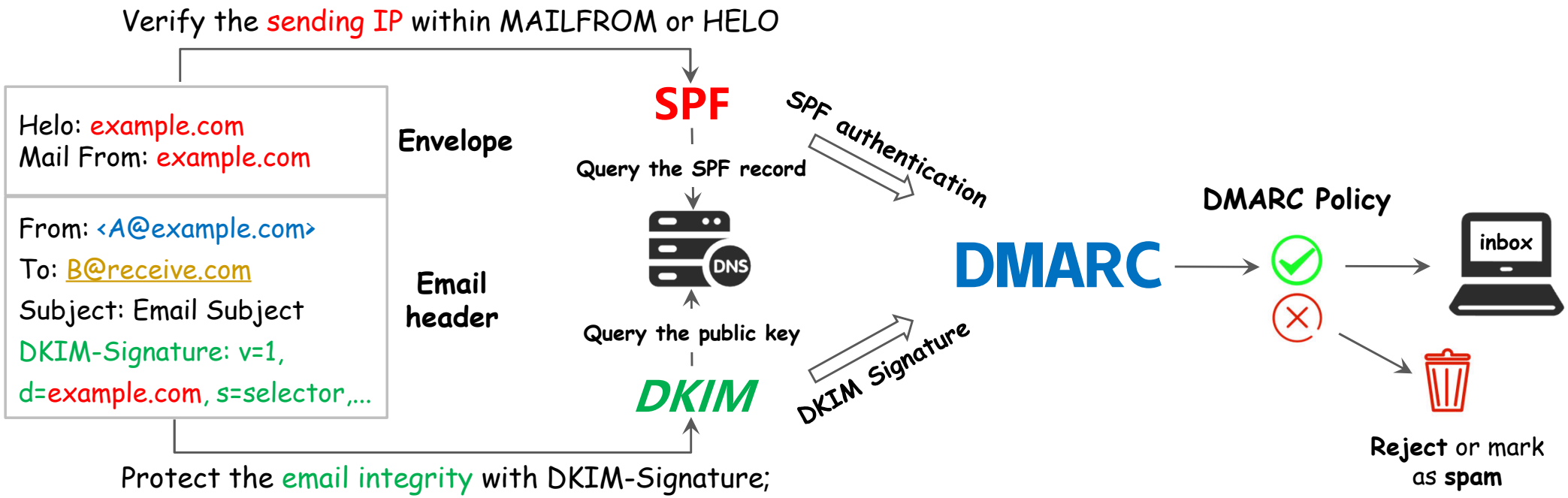
- **Email transmission**



- Original SMTP lacks authentication of the email sender;
- Various security extentions have been developed (SPF/DKIM/DMARC) ;

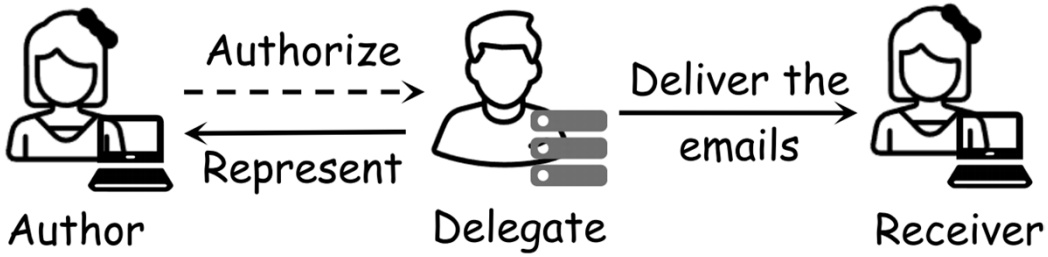
Background: Security Extensions

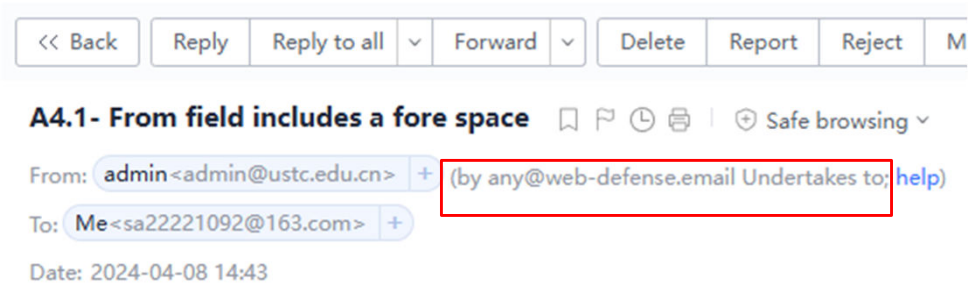
- **How security extensions work**



Background: Email Delegation Mechanism

Email sender authorizes other individual to represent them in dispatching emails.





RFC 5322 defines two header fields to identify:

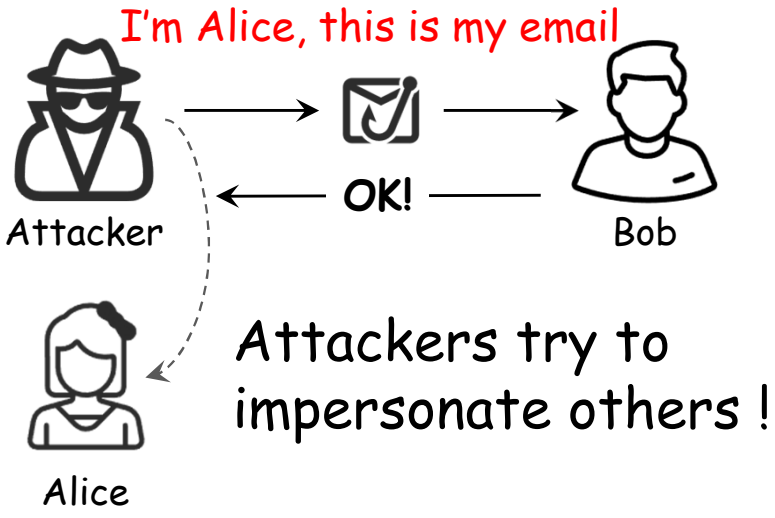
- Email Author (the From field)
- Email Delegate (the Sender field)

- Exposing the delegate is effective in recognizing potential phishing emails;
- The Delegate is concealed when consistent with email author;

The sender field is not validated by current security extensions.

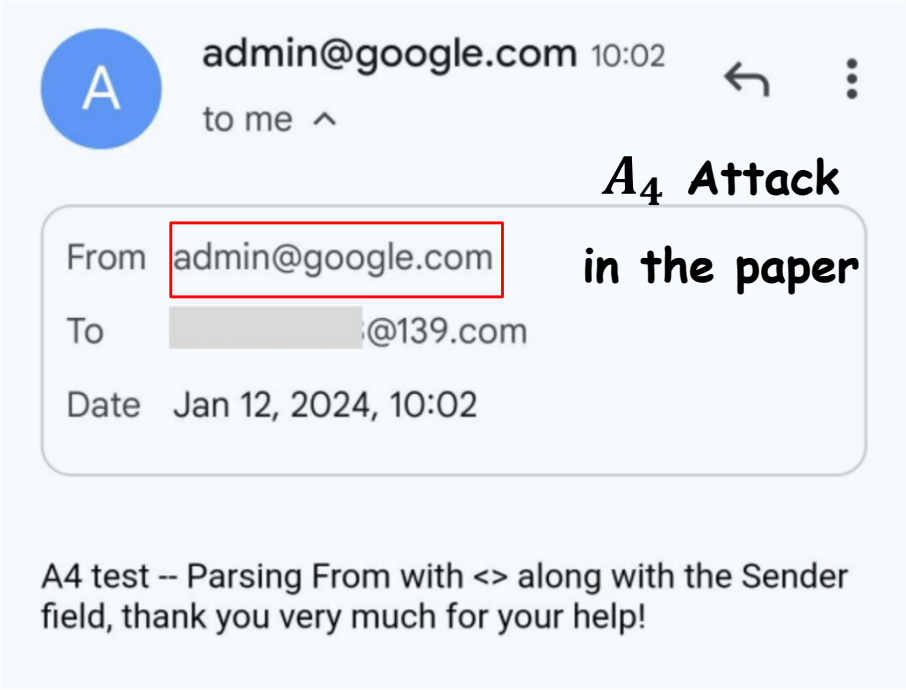
Email spoofing attack

- **Email spoofing attack**



Can the delegation mechanism being exploited in Email spoofing attacks?

- Mail Service Provider: @139.com
- Victim Client : Gmail app on Android

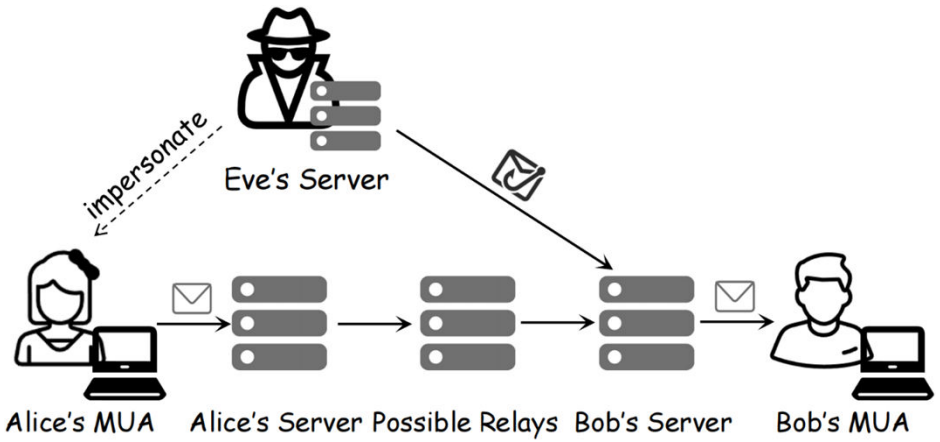


Outline

- Background
- **Attack model**
- Security Issues within Email Delegation
- Results
- Defensive measures

Attack Model

- The model includes **three entities:**
  - **Alice:** a trusted author;
  - **Bob**: email receiver;
  - **Eve**: Impersonate Alice to send emails;



- The model naturely **pass SPF/DKIM**:
  - Attackers will **not modify the SMTP** commands;
  - The sending domain is **fully controlled** by attackers;
  - Authentication Results are **not apparently displayed**;

HELO: attack.com

MAILFROM: <Eve@attack.com>

From: <Admin@legitimate.com\r\n>

Sender: ...

Outline

- Background
- Motivation
- **Security Issues within Email Delegation**
- Attack model and Results
- Defensive measures

Security issues: Overview

There are several **security issues** within the Delegation Mechanism:

- **Vul 1 - Protocol:** The Sender field is neglected by security protocols and can be arbitrarily spoofed by attackers.
- **Vul 2 - Implementation:** Various email providers and clients have different implementations of the Delegation Mechanism.

Our measurement: 16 providers * 20 clients

Vul-1: Fabricate the Sender field

- **Sender field fabrication**

HELO: attack.com

MAILFROM: <Eve@attack.com>

From: <Eve@attack.com\r\n>

To: <Bob@victim.com\r\n>

Sender: <**Admin@legitimate.com**\r\n>

The Sender field lacks authentication and can be **arbitrarily fabricated**.

- Spoofed Sender field is neglected by most providers
  - 5 providers modify the Sender field to be **consistent with MAILFROM**;
  - 11 providers leave the spoofed Sender field **unchanged** in emails.
  - Attackers can **fabricate the email Delegate** shown to the recipients;

163 网易免费邮 mail.163.com

Gmail

Vul-2: Inconsistent implementations

Key idea: Various email providers and clients adopt various implementations of the Delegation mechanism.

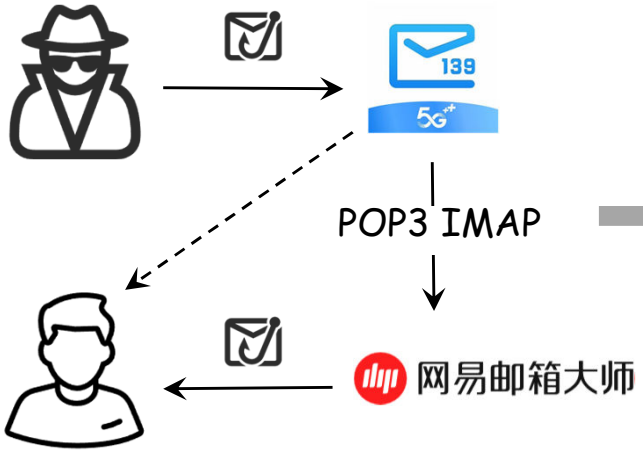
- **Web interfaces of providers**
  - Do not expose the Delegate (6)
    - NAVER Yandex ...
  - Expose the Delegate (5+3+2=10)
    - The Sender field: 163 网易免费邮 mail.163.com
    - Return-Path: Gmail
    - self-defined: sina 139 5G

- **Email clients**
  - Do not expose the Delegate (7)
    -
  - Expose the Delegate (13)
    - The Sender field: 网易邮箱大师
    - ~~Return-Path~~
    - ~~self-defined~~

    Unable to parse

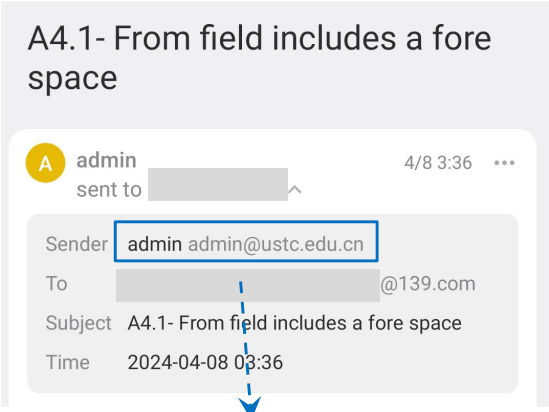
Attack Cases

Case 1: Receiving servers do not modify the spoofed Sender field, and the clients will display the wrong email Delegate.



- Display **self-defined field** as the Delegate;
- Display **the Sender field** as the Delegate;

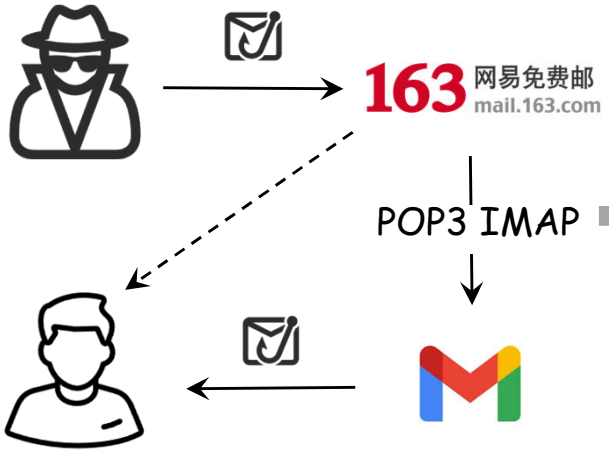
Exposing Attacker's address



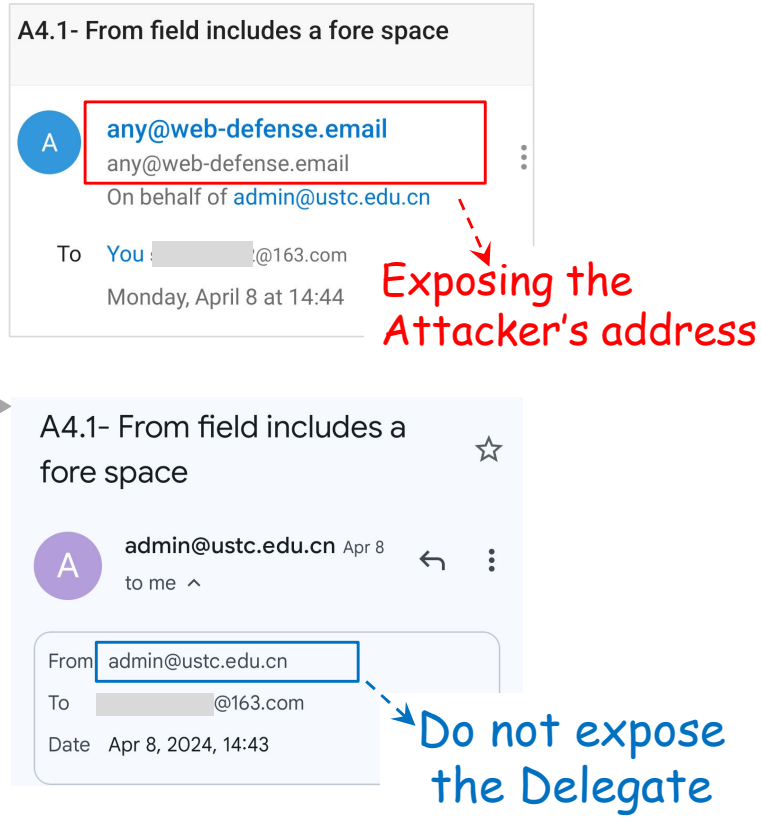
Delegate = email author

Attack Cases

Case 2: Receiving servers modify the Sender field to attacker's address, while clients do not show email Delegate.



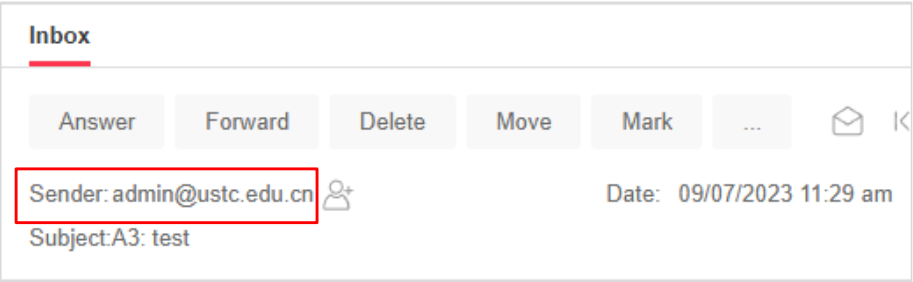
- Modify the Sender field to expose the attacker's address;
- Do not show the email Delegate to recipients;



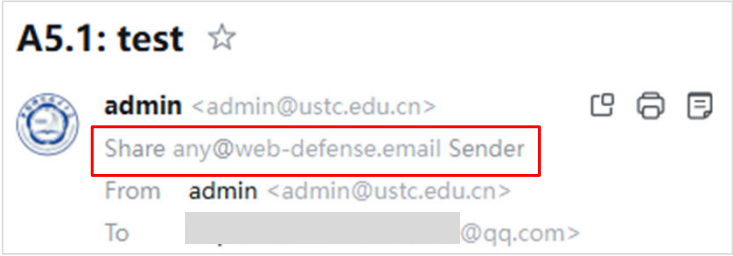
Attack Cases

Case 3: Web interfaces have some issues when exposing the Delegate

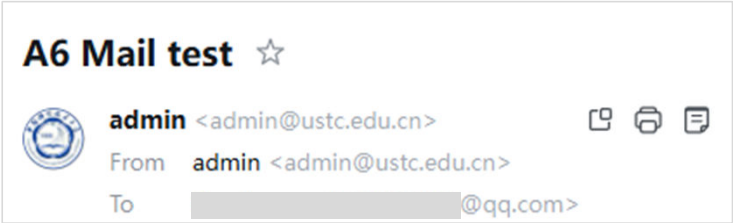
- Some providers do not adopt the policy to show the Delegate, raising potential risks in email spoofing (e.g., mailo.com).



- Some providers utilize spoofed Sender field as the Delagete (e.g., qq.com).



Test email without spoofed Sender field



Test email with spoofed Sender field

Outline

- Background
- Motivation
- Security Issues within Email Delegation
- **Results**
- Defensive measures

Evaluations

- 6 email spoofing attacks with comparison test;
- 16 email providers;
- **8 providers are affected**;

Service	A_1[1]		A_2		A_3		A_4		A_5		A_6	
	Sender	w/o Sender	Sender	w/o Sender	Sender	w/o Sender	Sender	w/o Sender	Sender	w/o Sender	Sender	w/o Sender
Gmail.com	×[2]	×	×	×	-	-	-	-	×	×	-	-
Outlook.com	-	-	-	-	-	-	-	-	-	-	-	-
163.com	×	×	✓	✓	×	×	✓	✓	×	×	✓	✓
Zoho.com	×	×	×	×	×	×	×	×	×	×	×	×
Yandex.com	-	-	-	-	×	×	-	-	-	-	-	-
Naver.com	×	×	-	-	×	×	-	-	×	×	×	×
QQ.com	✓	-	×	×	-	-	-	-	✓	✓	✓	✓
126.com	×	×	✓	✓	×	×	✓	✓	×	×	✓	✓
Rambler.com	-	-	-	-	-	-	-	-	-	-	-	-
Sohu.com	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Sina.com	-	-	-	-	-	-	-	-	-	-	-	-
139.com	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Mailo.com	✓	✓	×	×	✓	✓	✓	✓	✓	✓	-	-
Tutanota.com	-	-	-	-	-	-	-	-	-	-	-	-
Coremail.com	✓	✓	✓	✓	✓	✓	✓	✓	-	-	✓	✓
Yeah.net	×	×	✓	✓	×	×	✓	✓	×	×	✓	✓

[1] A_1 - A_6: Attacks 1 to 6 discussed in Section 6.1.
[2] "✓": attack emails reach the inbox; "×": the attack emails are rejected by the service provider; "-": the attack emails are recognized as spam.

- 20 mainstream email clients;
- **all clients are affected**;

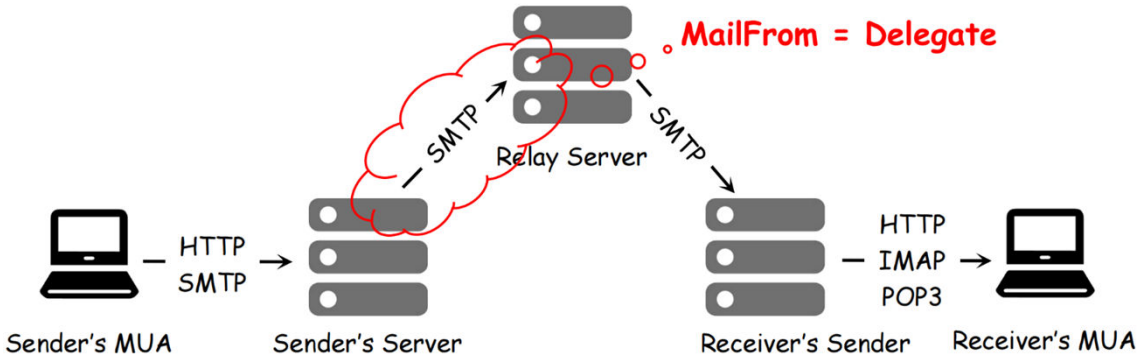
OS	Clients	Version	Exposing Delegate	Success Attack Types
Windows	Outlook	16.0.14332.20637	✓	A_1[1], A_3, A_4
	eM Client	9.2.2157	✓	A_1, A_3
	Win-Email	16005.14326.21904.0	✓	A_1, A_2, A_3, A_5, A_6
	Foxmail	7.2.25.245	✓	A_1, A_3, A_5, A_6
Linux	Thunderbird	115.7.0-1		A_2, A_3, A_6
	Evolution	3.50.0-1		A_3, A_6
	Mailspring	1.13.3		A_1, A_2, A_3, A_4
MacOS	Outlook	16.78.*	✓	A_1, A_2, A_5, A_6
	Apple Mail	Mac 14 (23B74)		A_6
	Foxmail	1.5.5	✓	A_1, A_3
	eM Client	9.2.2144.0	✓	A_1, A_3
iOS	Gmail	6.0.231127		A_1, A_2, A_3
	Apple Mail	iOS 17.1		A_1, A_3, A_5, A_6
	Outlook	4.2347.1	✓	A_1, A_2, A_3, A_5, A_6
	Netease	7.18.1	✓	A_1, A_2, A_3, A_4, A_5, A_6
	QQ	6.5.0	✓	A_1, A_3, A_6
Android	Gmail	2024.02.04.604829058		A_1, A_3, A_4
	Outlook	4.2347.4	✓	A_1, A_2, A_3, A_5, A_6
	Netease	7.18.4	✓	A_1, A_2, A_4, A_6
	QQ	6.5.1	✓	A_1, A_2, A_3, A_6

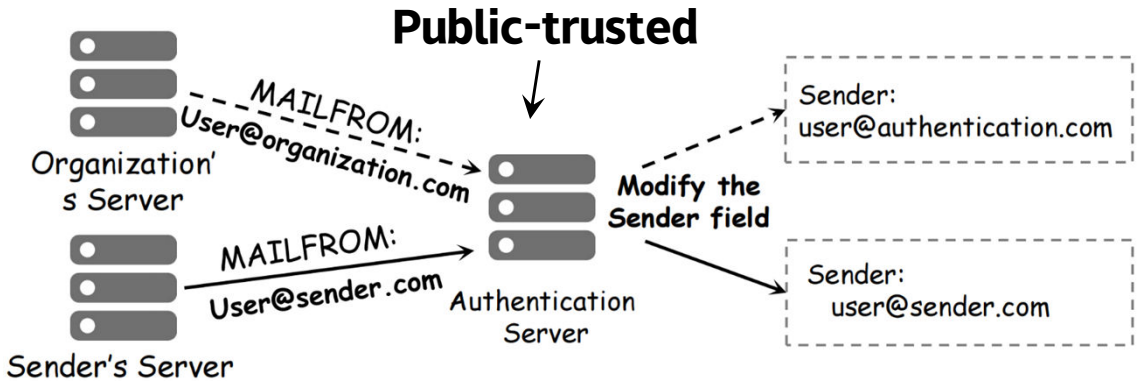
Outline

- Background
- Motivation
- Security Issues within Email Delegation
- Attack model and Results
- **Defensive measures**

Validation Scheme

- In email transmission,there exists **relay servers**;
- The Delegate is consistent with Mailfrom within the **first SMTP session**;
- Modify the spoofed Sender field during the First SMTP session;
- Considering realistic situations;





Security Suggestions

- **Suggestions for email clients**
  - To deploy the strategy to expose the email Delegate;
  - Parsing header fields that are used in web interfaces of mainstream providers as the Delegate;
  - Displaying a warning message when an email with a suspicious Sender field is shown to recipients;
- **Suggestions for email users**
  - Checking important emails more on web interfaces;
  - Trying replying to suspicious emails to observe the returning address;
  - Checking the raw email content when using clients such as Foxmail and Thunderbird;

usenix
THE ADVANCED
COMPUTING SYSTEMS
ASSOCIATION

Thank you!
Q&A

THE UNIVERSITY OF KANSAS