

Weak Links in Authentication Chains: A Large-scale Analysis of Email Sender Spoofing Attacks

Kaiwen Shen¹, Chuhan Wang¹, Minglei Guo, Xiaofeng Zheng, Chaoyi Lu,
Baojun Liu, Yuxuan Zhao, Shuang Hao, Haixin Duan, Qingfeng Pan, Min Yang

Email: skw17@mails.tsinghua.edu.cn

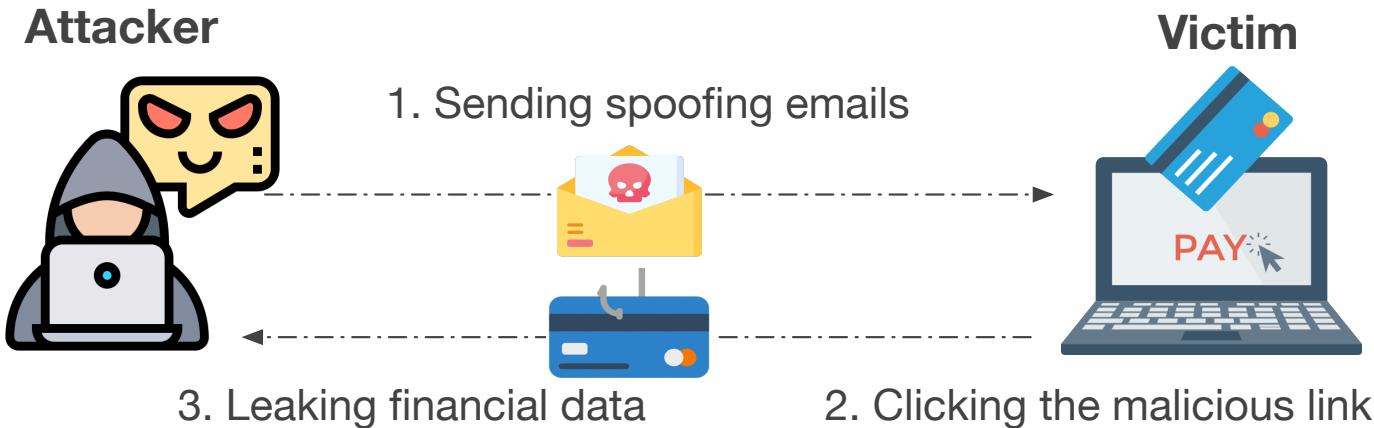


Coremail 论客



Email Spoofing Attacks

❖ How Email Spoofing Attacks Happen:



❖ Impact of Email Spoofing Attack Today

600%

Increase over 600% due to coronavirus pandemic (**COVID-19**).

*"The most devastating attacks by the most sophisticated attackers, almost always begin with the simple act of spearphishing." Jeh Johnson
Former Secretary, Department of Homeland Security*

\$5.3B → \$12.5B

FBI reports business have lost over \$12.5B. More than **double** in just over two years.

An Example of Our Email Spoofing Attack

SMTP DATA

HELO sender.com
MAIL FROM: <attack@sender.com>
RCPT TO : <victim@receiver.com>

From: <admin@xn--aypal-uye.com>
To: <victim@receiver.com>
Subject: Administrator's warning From Paypal.

Hello Dear Customer,

....

Check It Now



Displayed Email



Administrator's warning From PayPal

1 minute ago at 5:00 PM

From admin@paypal.com >



Hello Dear Customer,

Recently we have limited your account access. Please Check your account as soon as you can by Clicking the button below.

Check It Now



IDN homograph attack (A12): from paypal.com to iCloud

It's so hard to spot spoofing email !

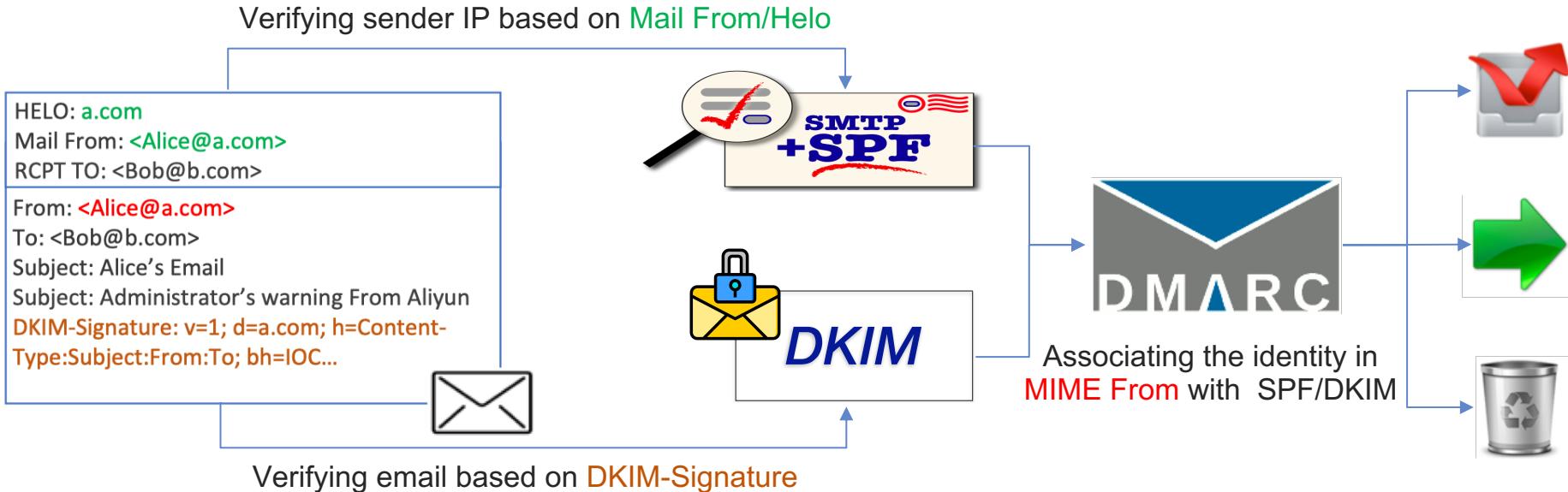
Email Spoofing Protections

Email Security Extension Protocol

- ❖ **Sender Policy Framework (SPF)**
 - Verifying **sender IP** based on Mail From/Helo
- ❖ **DomainKeys Identified Mail (DKIM)**
 - Verifying email based on **DKIM-Signature**
- ❖ **Domain-based Message Authentication, Reporting and Conformance (DMARC)**
 - ❖ Offering **a policy suggesting solution** to handle unverified emails
 - ❖ **Associating the identity** in MIME From with SPF/DKIM

Email Spoofing Protections

How Three Email Security Protocols Work:



Email Spoofing Protections

UI-level Spoofing Protection

- ❖ Sender Inconsistency Checks (SIC)

Administrator's warning From Outlook 

From: **admin** <admin@outlook.com> 
(Sent by oscar@attacker.com) 

Date: Monday, Nov 11, 2019 6:50 AM

To: victim <victim@outlook.com>

A spoofing email that fails the Sender Inconsistency Checks.

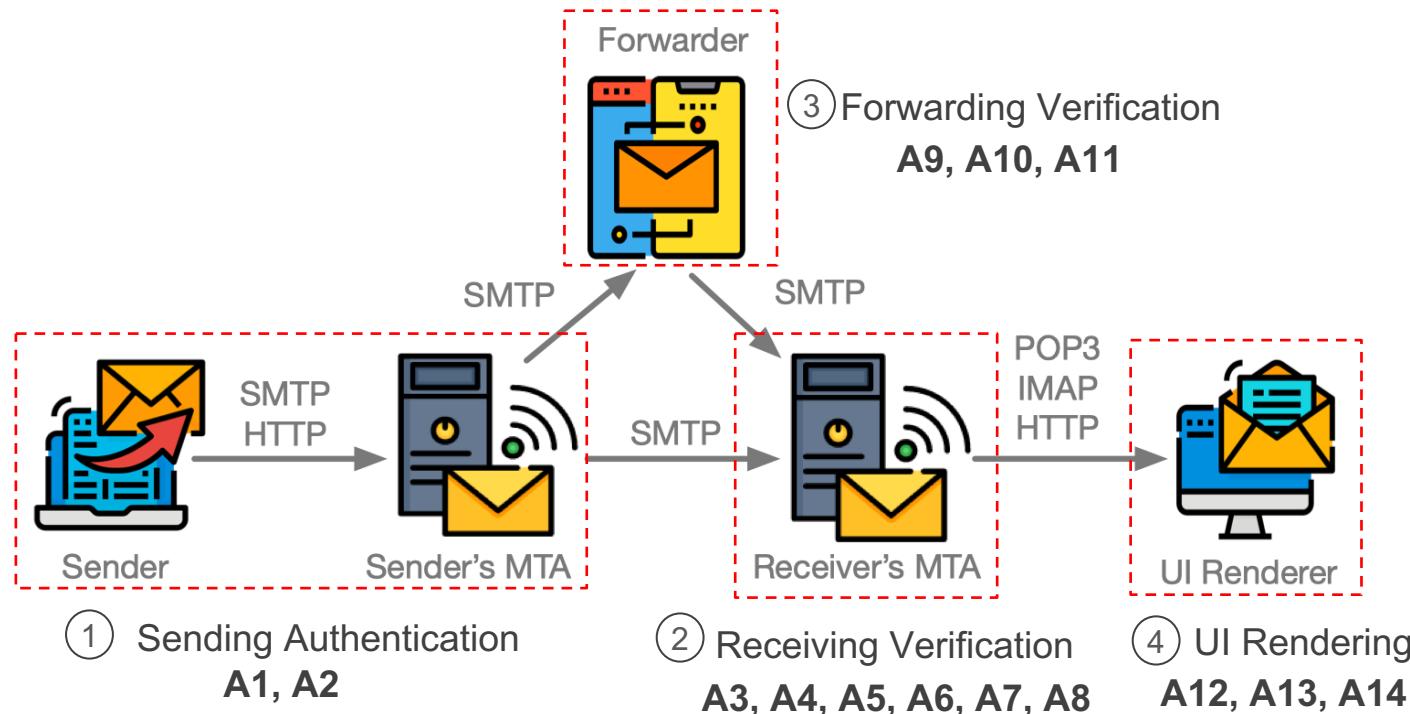
With these anti-spoofing protections,

Why email spoofing attack is still possible?



Our Works

- ❖ **Goal:** Analyze four critical stages of authentication chain.
- ❖ **Finds:** **14** email spoofing attacks, including **9** new attacks.



Measurement and Evaluation in the Wild

- ❖ A large-scale experiment on **30** popular email services and **23** email clients.

Email Services	Protocols Deployment			UI Protections SIC	Weaknesses in Four Stages of Email Flows			
	SPF	DKIM	DMARC		Sending	Receiving	Forwarding	UI Rendering
Gmail.com	✓	✓	✓	✓		A ₆		A ₁₂
Zoho.com	✓	✓	✓	✓	A ₂	A ₄	A ₁₁	A ₁₃
iCloud.com	✓	✓	✓		A ₂	A ₄ , A ₇	A ₉	A ₁₂
Outlook.com	✓	✓	✓		A ₂	A ₇	A ₉	A ₁₄
Mail.ru	✓	✓	✓			A ₄		A ₁₂
Yahoo.com	✓	✓	✓		A ₂	A ₃ , A ₇	A ₁₀	A ₁₄
QQ.com	✓	✓	✓	✓	A ₂	A ₅		A ₁₃ , A ₁₄
139.com	✓		✓	✓		A ₄		A ₁₃
Sohu.com	✓				A ₂	A ₄ , A ₅	A ₉	A ₁₃
Sina.com	✓				A ₂	A ₃ , A ₄ , A ₅ , A ₈		A ₁₃ , A ₁₄
Tom.com	✓	✓	✓		A ₂		A ₉	
Yeah.com	✓	✓	✓	✓	A ₂	A ₃ , A ₄ , A ₅ , A ₇ , A ₈	A ₉	A ₁₂ , A ₁₃ , A ₁₄
126.com	✓	✓	✓	✓	A ₂	A ₃ , A ₄ , A ₅ , A ₈	A ₉	A ₁₂ , A ₁₃ , A ₁₄
163.com	✓	✓	✓	✓	A ₂	A ₃ , A ₄ , A ₅ , A ₇ , A ₈	A ₉	A ₁₂ , A ₁₃ , A ₁₄
Aol.com	✓	✓	✓		A ₂	A ₅ , A ₇		A ₁₄
Yandex.com	✓	✓	✓			A ₃ , A ₄ , A ₆ , A ₇ , A ₈	A ₉	A ₁₄
Rambler.ru	✓	✓	✓		A ₂	A ₃		
Naver.com	✓	✓	✓		A ₂	A ₄ , A ₅ , A ₈		
21cn.com	✓				A ₂	A ₄ , A ₅	A ₉	
Onet.pl	✓				A ₂	A ₄ , A ₅		
Cock.li	✓	✓			A ₂	A ₃ , A ₄		A ₁₃ , A ₁₂
Daum.net	✓		✓			A ₅		
Hushmail.com	✓	✓	✓			A ₃ , A ₄ , A ₈		A ₁₂
Exmail.qq.com	✓	✓	✓	✓	A ₂	A ₅		A ₁₄
Coremail.com	✓	✓	✓	✓	A ₂	A ₈	A ₉	
Office 365	✓	✓	✓	✓	A ₂	A ₄	A ₉ , A ₁₀ , A ₁₁	A ₁₄
Alibaba Cloud	✓	✓	✓	✓	A ₂	A ₃ , A ₄ , A ₅ , A ₈	A ₁₀	A ₁₃
Zimbra	✓	✓	✓	✓	A ₁ , A ₂	A ₃ , A ₅ , A ₈	A ₉	A ₁₂ , A ₁₃
EwoMail	✓	✓	✓	✓	A ₂	A ₃ , A ₄ , A ₈		A ₁₃
Roundcube	✓	✓	✓		A ₁ , A ₂	A ₃ , A ₄ , A ₈		A ₁₂

OS	Clients	SIC	Weaknesses
Windows	Foxmail	✓	A ₆ , A ₇ , A ₁₃ , A ₁₄
	Outlook	✓	A ₆ , A ₁₃
	eM Client	✓	A ₆ , A ₁₂
	Thunderbird		A ₆ , A ₁₃ , A ₁₄
MacOS	Windows Mail		A ₆ , A ₇ , A ₁₃ , A ₁₄
	Foxmail		A ₆ , A ₁₃
	Outlook	✓	A ₆ , A ₁₃
	eM Client	✓	A ₆ , A ₇ , A ₁₂ , A ₁₃ , A ₁₄
	Thunderbird		A ₆ , A ₁₃ , A ₁₄
Linux	Apple Mail		A ₆ , A ₁₃ , A ₁₄
	Thunderbird		A ₆ , A ₁₃
	Mailspring		A ₆ , A ₁₃ , A ₁₄
	Claws Mail		A ₆ , A ₁₄
	Evolution		A ₆ , A ₁₃ , A ₁₄
Android	Sylpheed		A ₆ , A ₁₃ , A ₁₄
	Gmail		A ₆ , A ₁₃
	QQ Mail	✓	A ₆ , A ₁₃ , A ₁₄
	NetEase Mail		A ₆ , A ₁₂ , A ₁₃
iOS	Outlook	✓	A ₆ , A ₁₃
	Mail.app		A ₆ , A ₇ , A ₁₃ , A ₁₄
	QQ Mail	✓	A ₆ , A ₁₃
	NetEase Mail		A ₆ , A ₁₂ , A ₁₃
	Outlook	✓	A ₆ , A ₁₃

Measurement and Evaluation in the Wild



Apple Mail

阿里邮箱

Email Calendar

Administrator's warning From Aliyun!

From: admin <admin@aliyun.com>
To: victim

Did you really receive an email from the admin@aliyun.com?

QQ邮箱 mail.qq.com

Administrator's warning From 163!

From: <admin@163.com>
Date: March 22, 2019 17:32 (Friday)
To: victim <victim@qq.com>

Did you really receive an email from the admin@163.com?

163 网易免费邮 mail.163.com

首页 通讯录 应用

Administrator's warning From QQ!

From: admin <admin@qq.com>
To: victim <victim@163.com>
Date: April 16, 2021, 19:47 (Friday)

Did you really receive an email from the admin@qq.com?

Gmail

Compose

Inbox

Starred Snoozed Sent Drafts More

Administrator's warning From Aliyun!

From: admin@aliyun.com
to victim

Did you really receive an email from the admin@aliyun.com?

Administrator's warning From PayPal

1 minute ago at 5:00 PM
From admin@paypal.com

Did you really receive an email from the admin@PayPal.com?

PayPal

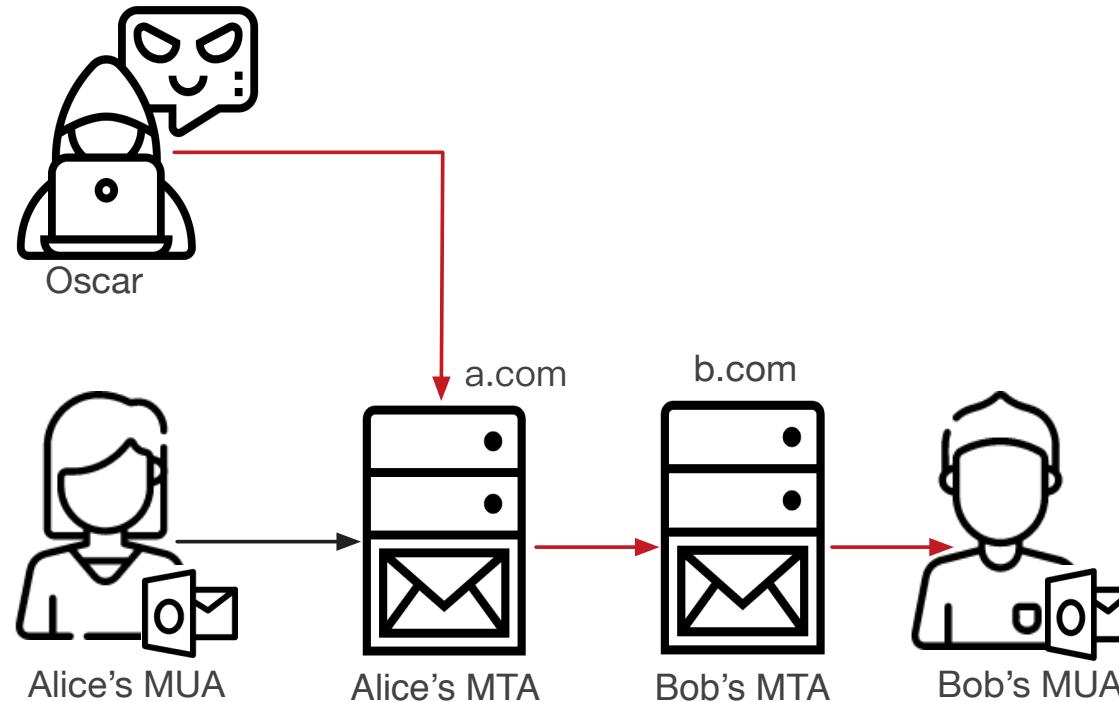
All of tested email services are **vulnerable** to certain types of attacks.

Attacks

Three Types of Attack Models

a. Shared MTA Attack

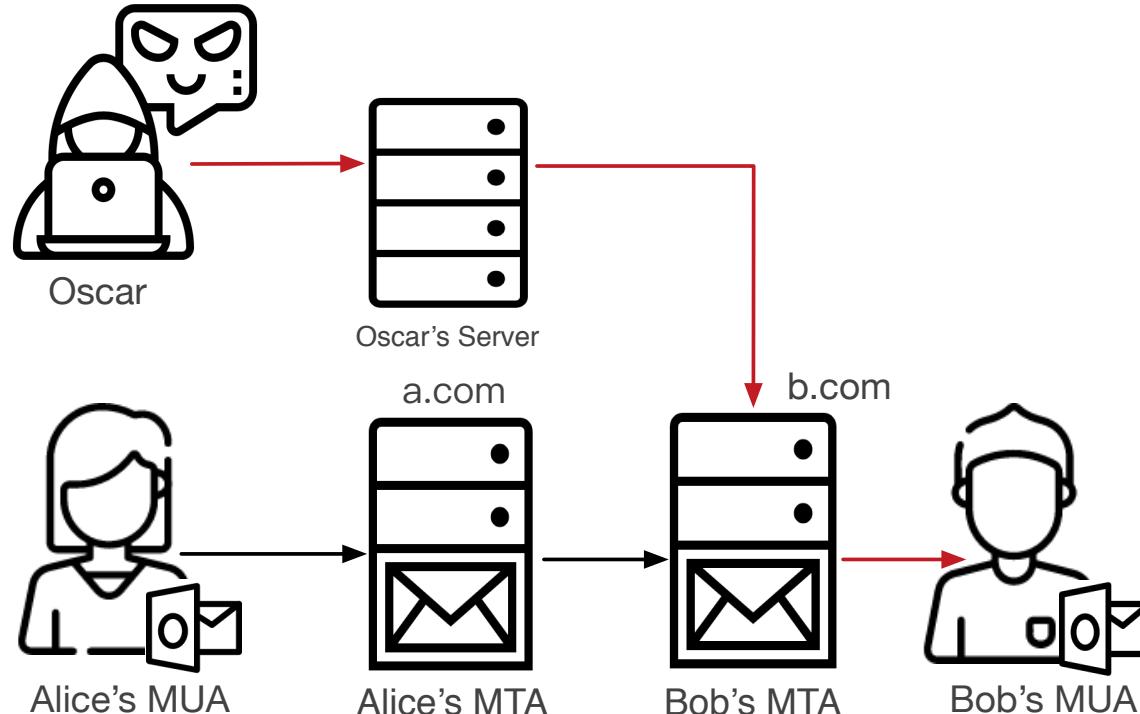
Oscar@a.com sends spoofing email as Alice@a.com with the a.com MTA



Three Types of Attack Models

b. Direct MTA Attack

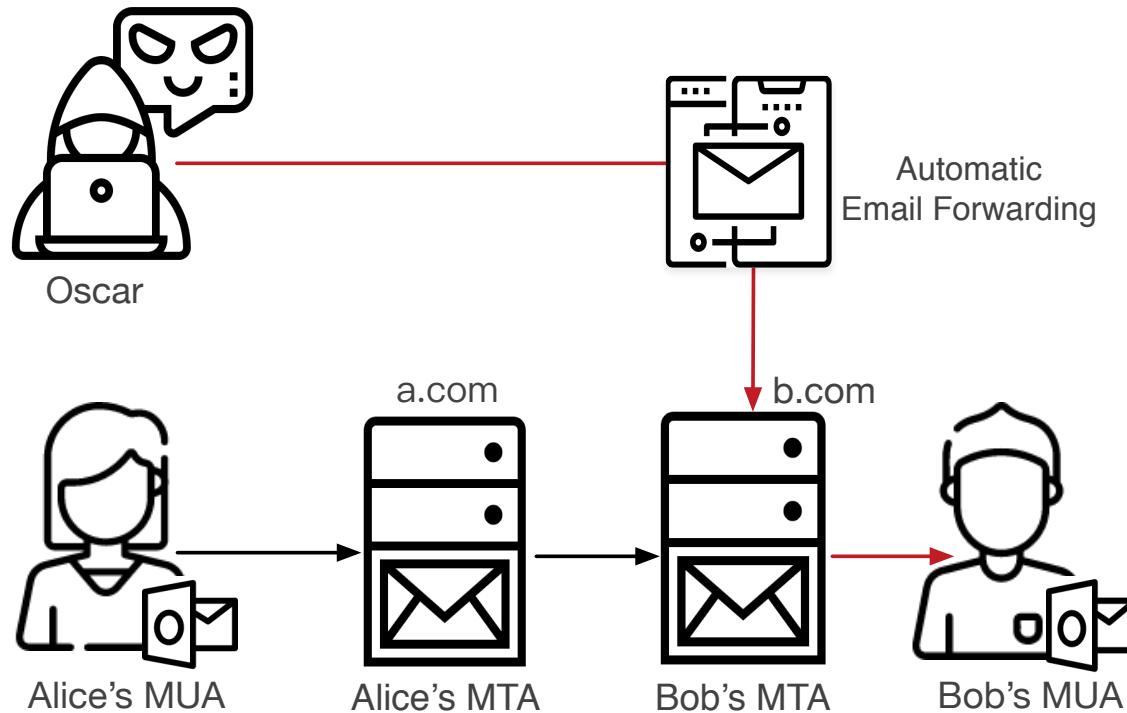
Oscar sends spoofing email through his own email server.



Three Types of Attack Models

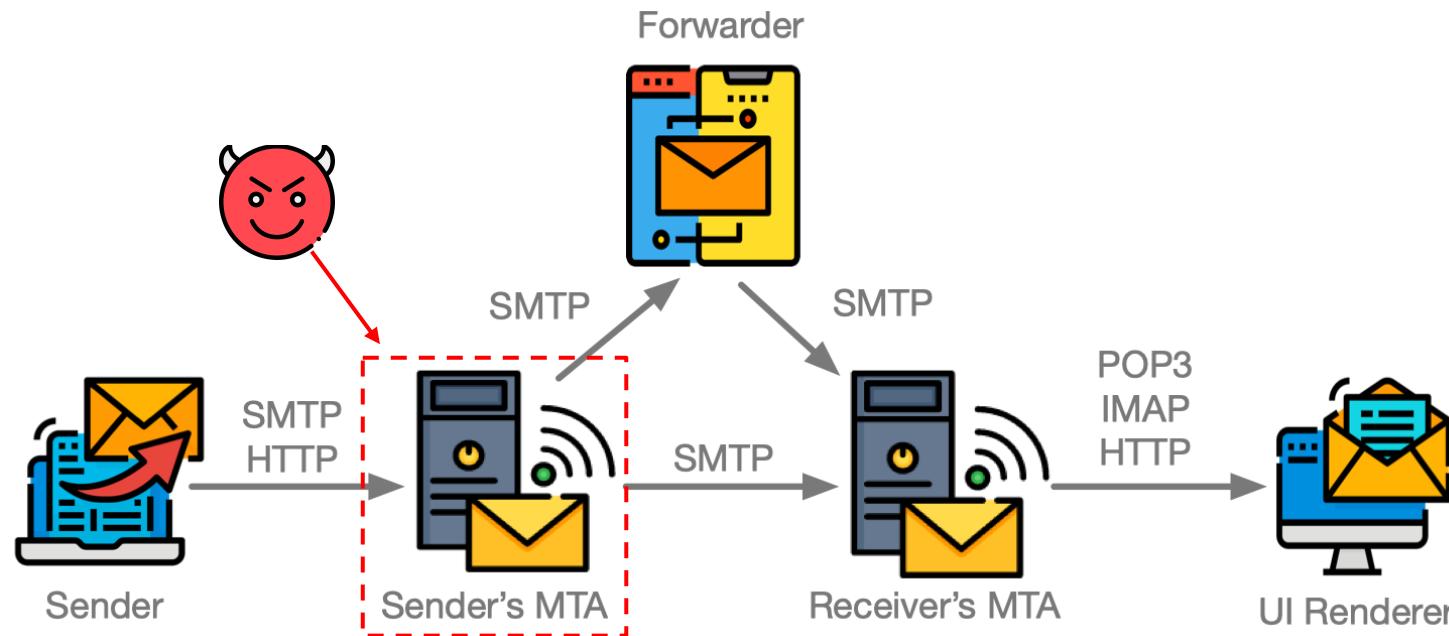
c. Forward MTA Attack

Oscar abuses email forwarding service to send spoofing emails.



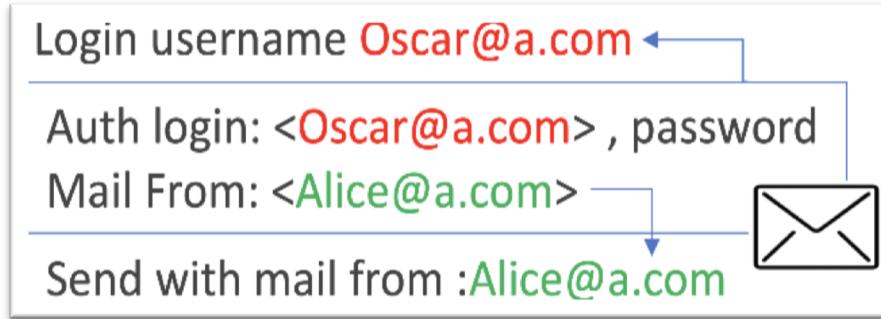
Attacks in Email Sending Authentication

- ❖ **Successful Attack:** modifying Auth Username, Mail From, From arbitrarily.
- ❖ **Benefit :** abusing IP reputation of well-known email services.



Attacks in Email Sending Authentication

- ❖ Auth Username ≠ Mail From (A1)

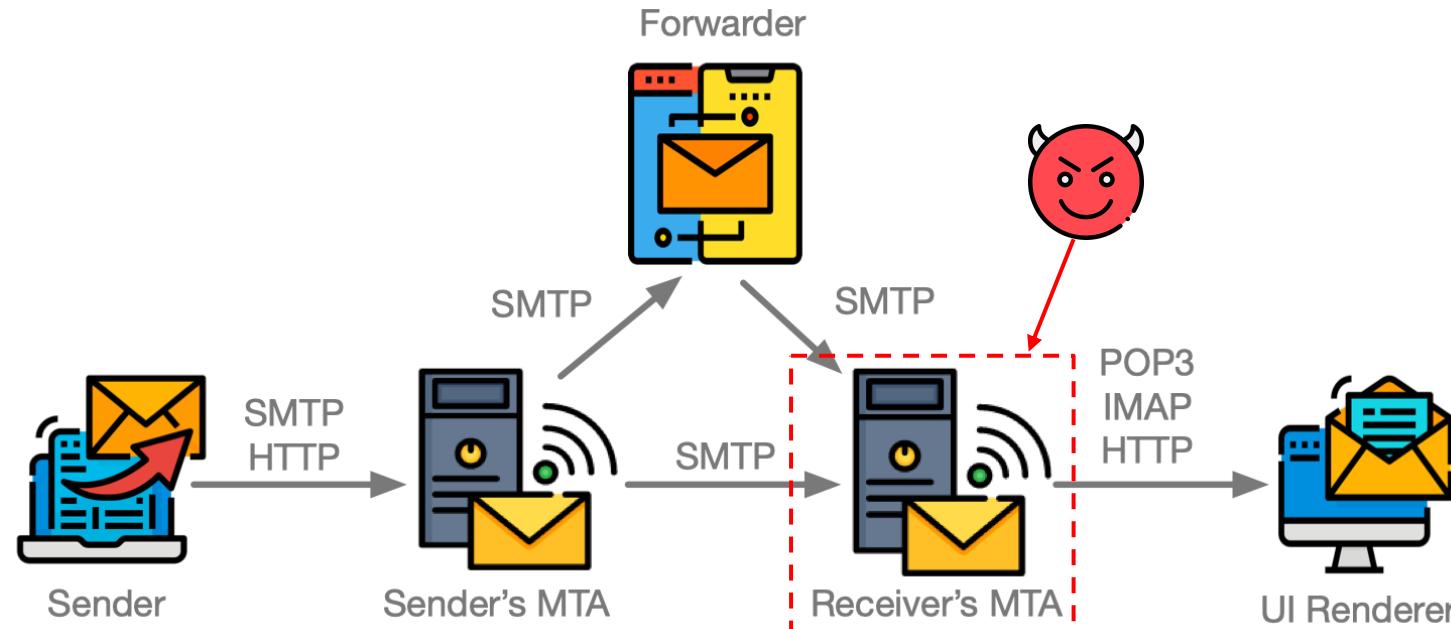


- ❖ Mail From ≠ From (A2)



Attacks in Email Receiving Verification

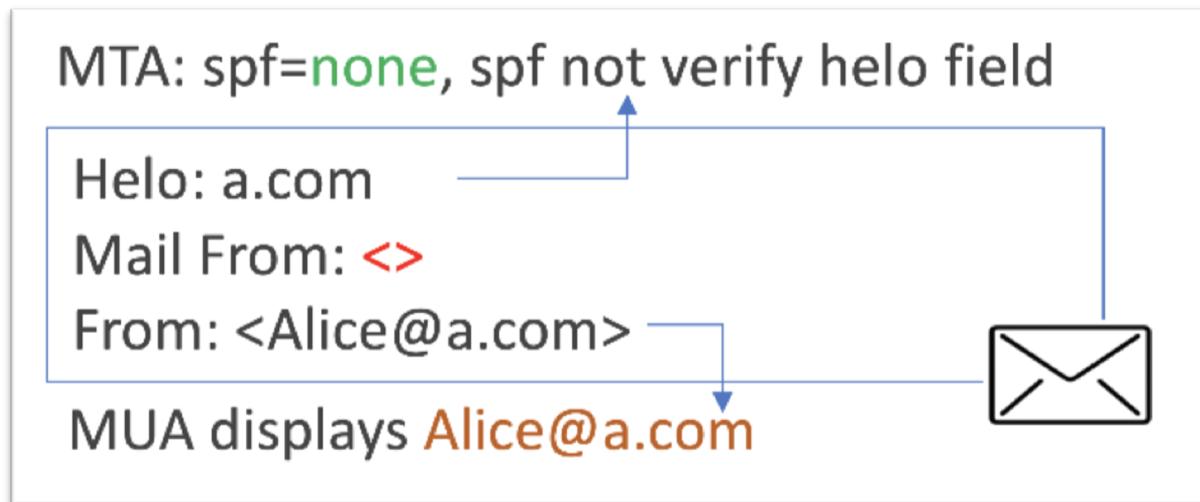
- ❖ **Successful Attack:** bypassing SPF, DKIM and DMARC.
- ❖ **Benefit:** hard to spot spoofing email passing three security protocols.



Attacks in Email Receiving Verification

Empty Mail From (A3)

- ❖ RFC 5321: Empty mail from is allowed to prevent bounce loop-back
- ❖ RFC 7208: Use helo field as an alternative, if mail from is empty



Empty Mail From attack bypassing the SPF verification

Attacks in Email Receiving Verification

Inconsistent Parsing of Ambiguous Emails

- ❖ Multiple from headers(A4)

MTA: dmarc=pass, DMARC verifies attack.com

From: <Oscar@attack.com>
From: <Alice@a.com>

MUA displays **Alice@a.com**

MTA: dmarc=pass, DMARC verifies attack.com

From: <Oscar@attack.com>
From: <Alice@a.com>

MUA displays **Alice@a.com**

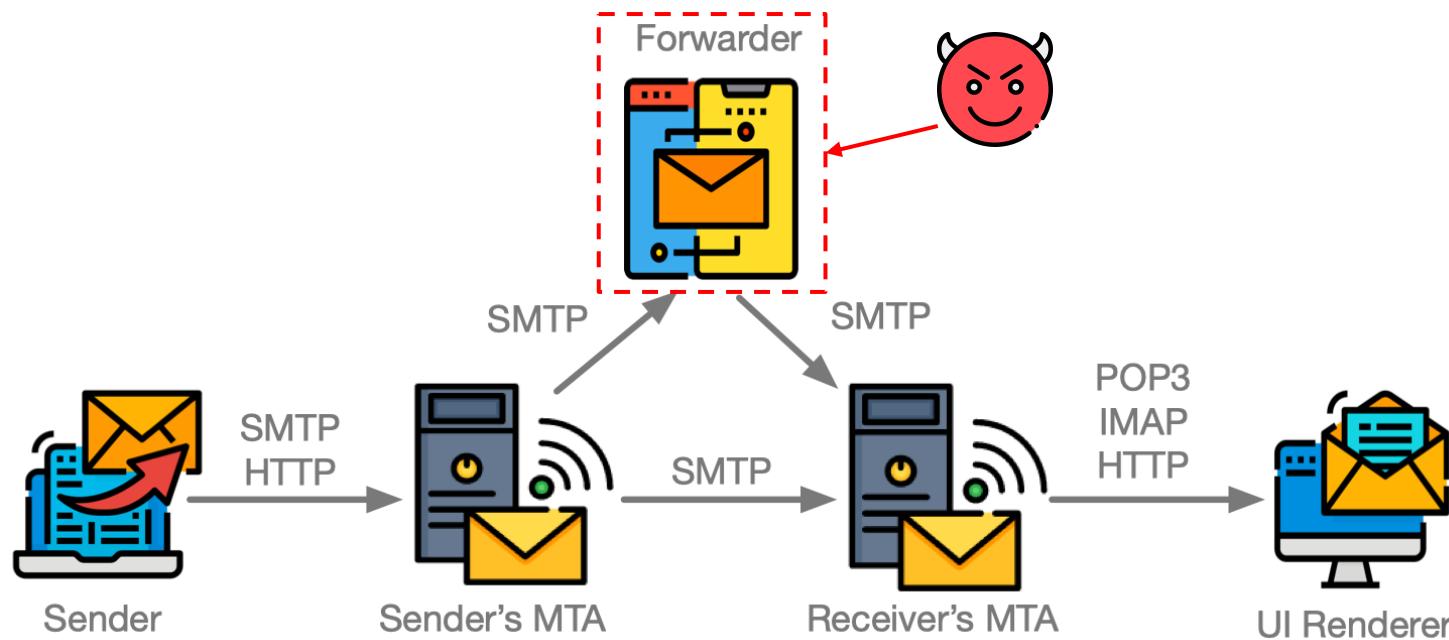
Ordinary multiple From attack

Multiple From attack with spaces

Attacks in Email Forwarding Verification

Successful Attack:

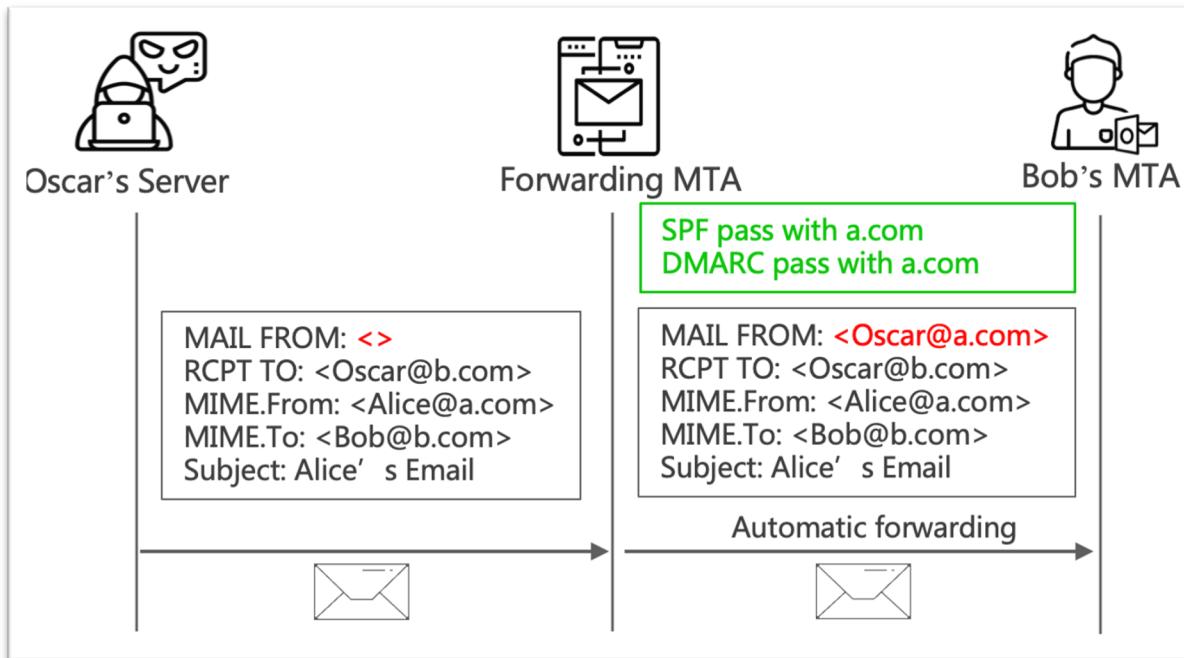
- ❖ Freely configure without authentication verification
- ❖ A higher security endorsement



Attacks in Email Forwarding Verification

Unauthorized Forwarding Attack (A9)

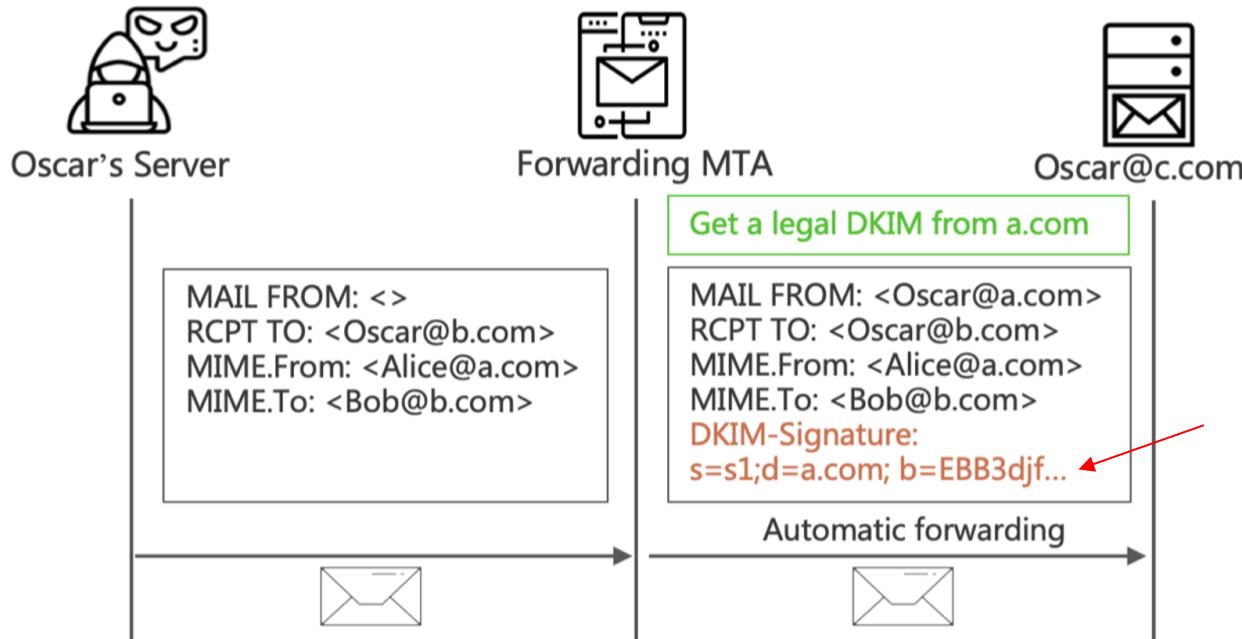
- ❖ Abusing trusted IP: Exploiting forwarding service to bypass SPF and DMARC



Attacks in Email Forwarding Verification

DKIM-Signature Fraud Attack (A10)

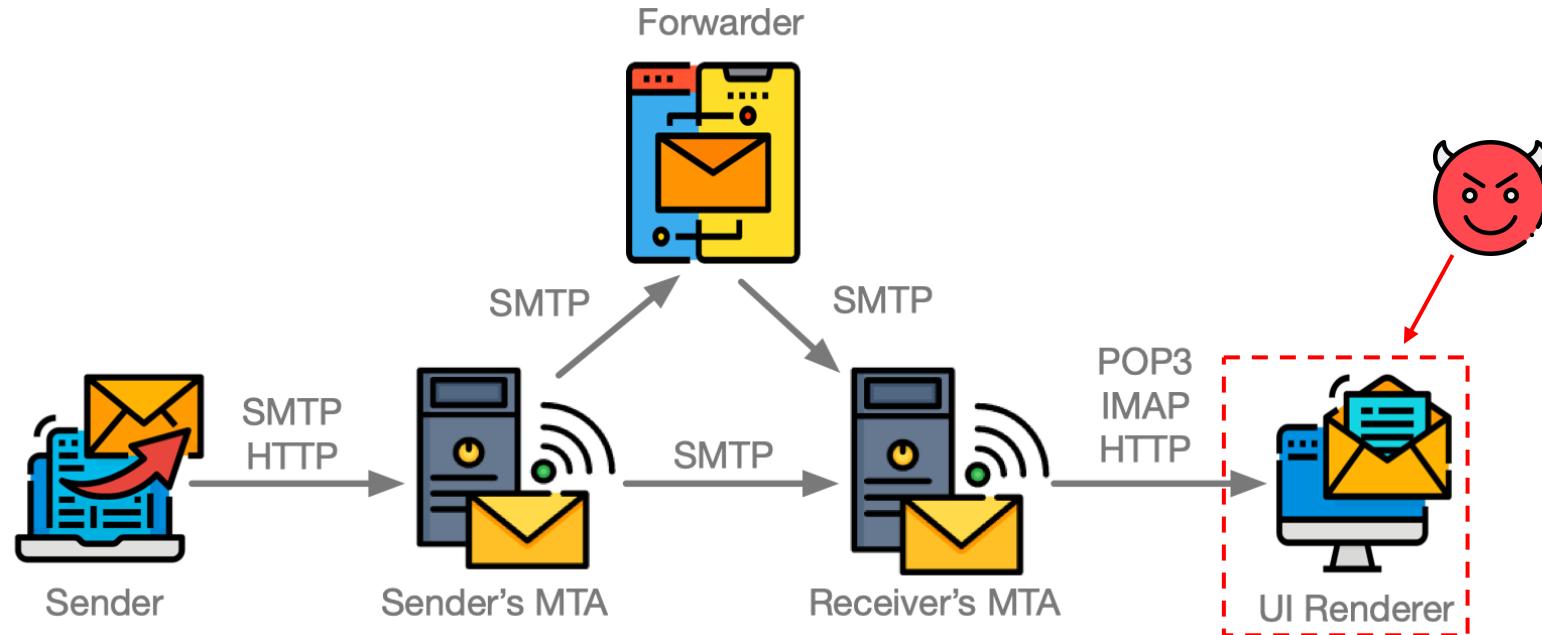
- ❖ A higher security endorsement : obtain a legal DKIM-Signature



Attacks in Email UI Rendering

Successful Attack:

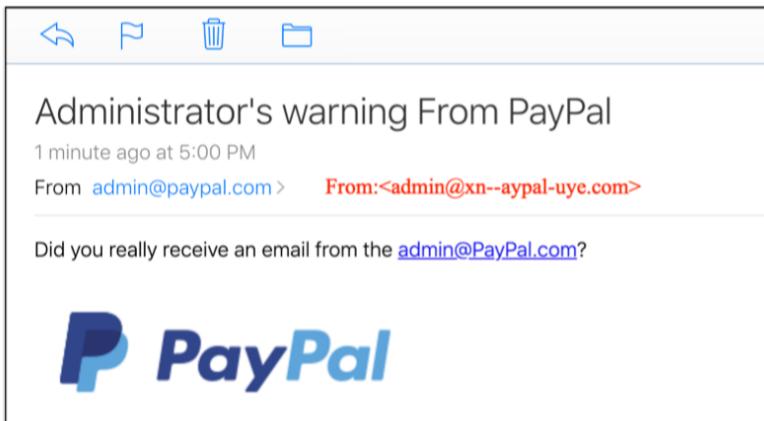
- ❖ The displayed address is inconsistent with the real one.
- ❖ No any security alerts on the MUA.



Attacks in Email UI Rendering

New Challenge : International Email

- ❖ Internationalized domain names (**IDN**) + email address internationalization (**EAI**)
- ❖ Allow **Unicode** characters in email address



IDN homograph attack (A12)

admin@gm@ail.com ==> admin@gmail.com

Missing UI Rendering Attack (A13)

\u202emoc.a@\u202dalice ==> Alice@a.com

Right-to-left Override Attack (A14)

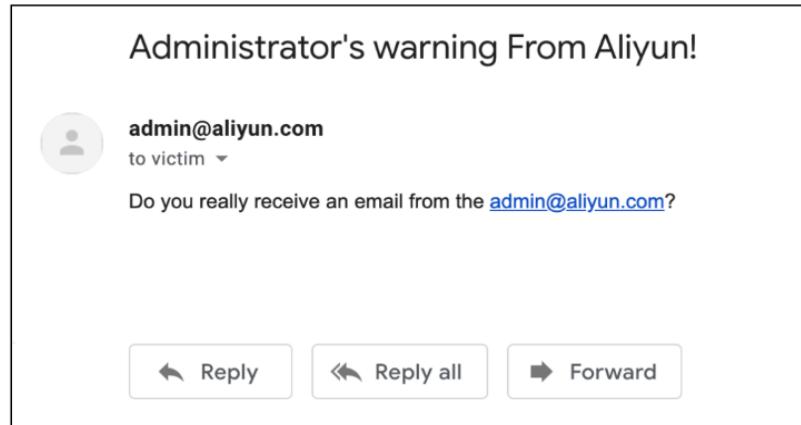
Combined Attack

Limitations on a single attack:

- Some attacks (e.g., A2, A3) do not bypass all protections.
- Most vendors have fixed the attacks (bypassing all SPF,DKIM,DMARC and SIC).

Combined Attack:

- More realistic emails (bypassing all prevalent email security protocols).



(a) Gmail's Web UI does not display any spoofing alerts

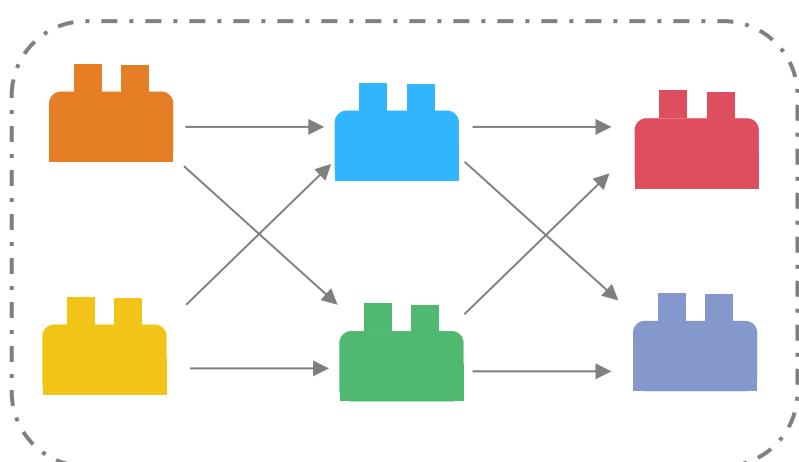
Message ID	<5dcf2150.1c69fb81.4f281.9f87SMTPIN_ADDED_MISSING@mx.google.com>
Created at:	Sat, Nov 16, 2019 at 5:42 AM (Delivered after 1432 seconds)
From:	admin@aliyun.com
To:	victim@gmail.com
Subject:	Administrator's warning From Aliyun!
SPF:	PASS with IP 2402:f000:1e:4000:b061:551e:2cec:b6d Learn more
DKIM:	'PASS' with domain aliyun.com Learn more
DMARC:	'PASS' Learn more

(b) The spoofing email passes all email security protocol verification

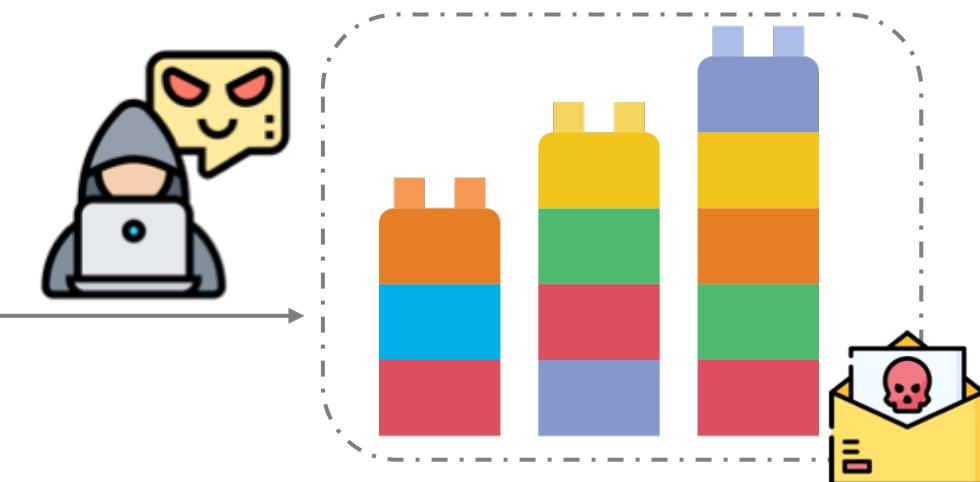
A example to impersonate admin@aliyun.com on Gmail.

Combined Attacks

- ❖ Numerous feasible combined attacks by combining **3** types of attack models and **14** attack techniques in the **4** authentication stages.



Different Attack Models/Techniques

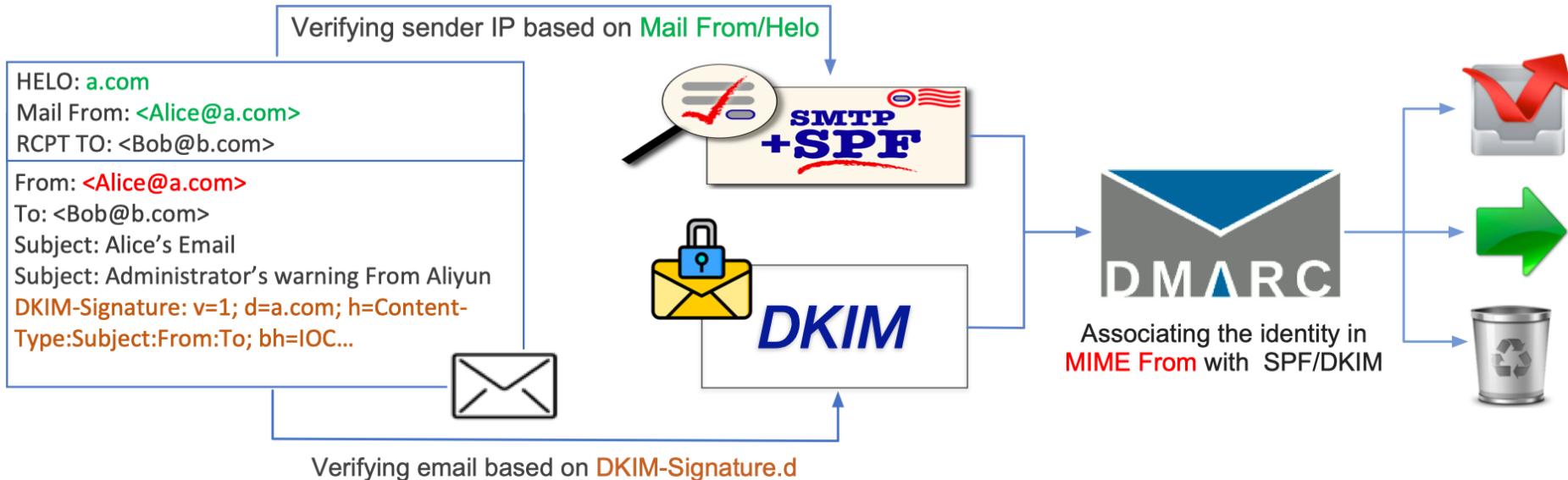


Combined Spoofing Attacks

Weak Links in Authentication Chains

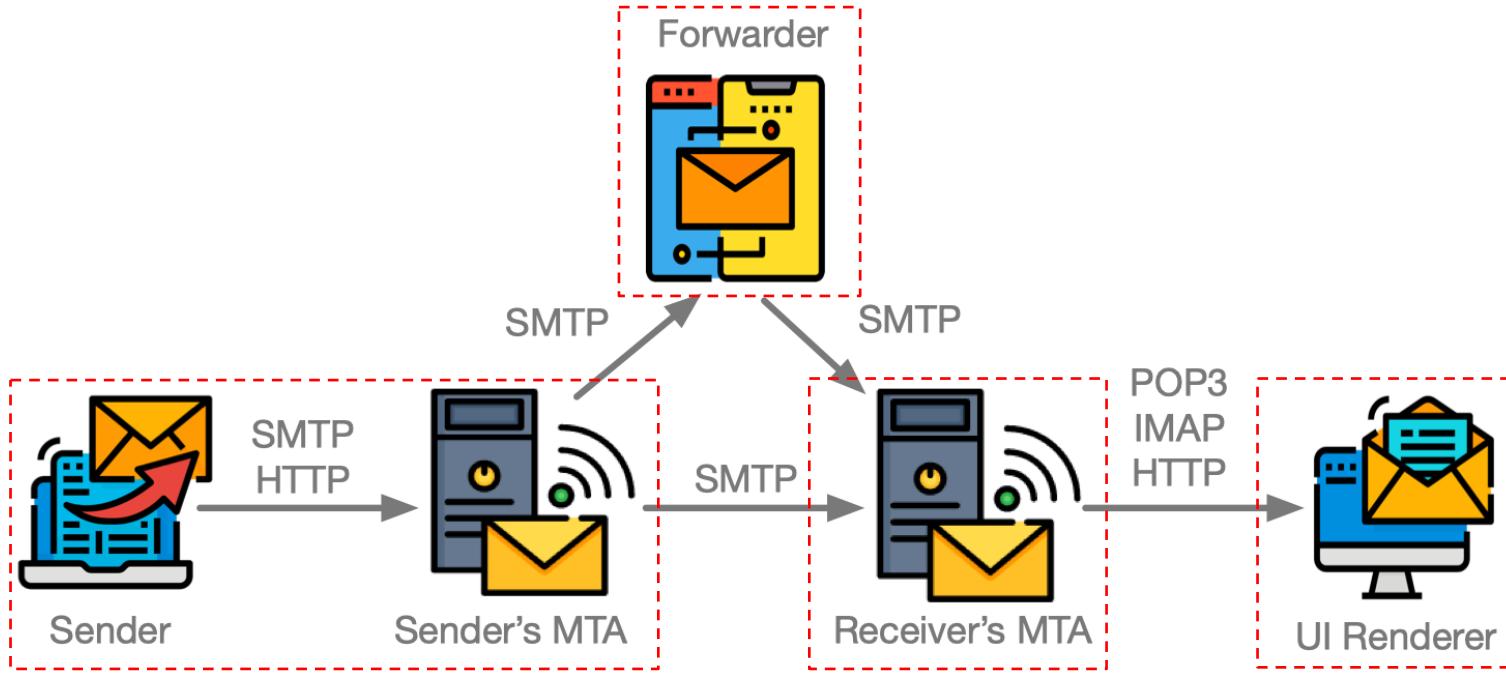
Weak Links among Multi-protocols

- ❖ Spoofing attacks still succeed due to the inconsistency of entities protected by different protocols.



Weak Links among Multi-roles

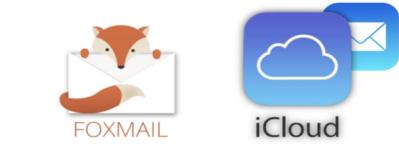
- ❖ Four different roles: **senders**, **receivers**, **forwarders** and **UI renderers**.
- ❖ The specifications do not state any clear responsibilities of four roles.
- ❖ Any failed part can break the whole chain-based defense.



Weak Links among Multi-services

- ❖ Different email services have different configurations and implementation procedures.
- ❖ Numerous email components deviate from RFC specifications while dealing with ambiguous header.

The inconsistency among different services creates security threats.



Mitigation

Responsible Disclosure

- ❖ Helping Email vendors eliminate the detected threats.
 - Vendors have 10 months to mitigate it before this paper is published.



Mitigation and Solution

❖ UI Notification:

NoSpoofing: a chrome extension for Gmail.



NoSpoofing

提供方: wchhlbt

★★★★★ 1 | 社交与通讯

Administrator's warning From Aliyun!

admin@aliyun.com to victim ▾

Do you really receive a mail from admin@aliyun.com?

⚠ The email is suspected to be sent from <attacker@attack.com>.

Abnormal Behaviors: **Mail From header is inconsistent with From header.**
The verified domains of the three protocols are different.

Mail From: attacker@attack.com
From: admin@aliyun.com
to: victim@gmail.com
date: Nov 16, 2019, 5:42 AM
subject: Administrator's warning From Aliyun!
SPF: "pass" with domain attack.com
DKIM: "pass" with domain aliyun.com
DMARC: "pass" with domain aliyun.com

Reply

An example of UI notification against the combined attack

<https://chrome.google.com/webstore/detail/nospoofing/ehidaopjcnapdglbbbjgeoagpophfjn>

Mitigation and Solution

❖ Evaluation Tools:

EsSpoofing: helping email administrators to evaluate and strengthen their security.

Today (11 message(s))		
<input type="checkbox"/>		test@moc.tset [Warning] Maybe you are vulnerable to the A14 attack!
<input type="checkbox"/>		nislemail123... [Warning] Maybe you are vulnerable to the A13 attack!
<input type="checkbox"/>		admin [Warning] Maybe you are vulnerable to the A2 attack!
<input type="checkbox"/>		admin, nislem... [Warning] Maybe you are vulnerable to the A5 attack!
<input type="checkbox"/>		admin [Warning] Maybe you are vulnerable to the A4 attack!
<input type="checkbox"/>		nislemail123, ... [Warning] Maybe you are vulnerable to the A5 attack!
<input type="checkbox"/>		nislemail123 [Warning] Maybe you are vulnerable to the A4 attack!
<input type="checkbox"/>		admin [Warning] Maybe you are vulnerable to the A12 attack!
<input type="checkbox"/>		@test.com@q... [Warning] Maybe you are vulnerable to the A14 attack!
<input type="checkbox"/>		alipay [Warning] Maybe you are vulnerable to the A12 attack!

[Warning] Maybe you are vulnerable to the A12 attack!

From: admin@alipay.com
(Forward by nislemail123@yeah.net)
Time: 2024-02-20 10:00:00
To:

INFO:

This is an evaluation email sent by EmailTestTool to help email administrators to evaluate and strengthen their security.
If you see this email, it means that you may be vulnerable to the email spoofing attacks.
This email uses the IDN Homograph Attack(A12).

How to fix it:

For the IDN IDN Homograph Attack(A12): You can only display the original address with Punycode character, if a domain label contains characters from multiple different languages.

More Details:

More email header details are provided to help you to configure the corresponding email filtering strategy.

MAIL From: nislemail123@yeah.net
Content-Type: multipart/mixed; boundary="=====0104020709624520490===="
MIME-Version: 1.0
To:
From: admin@xn--80aa1cn6g67a.com
Subject: [Warning] Maybe you are vulnerable to the A12 attack!

An example of using this tool to evaluate the security of target email system.

<https://github.com/mo-xiaoxi/ESpoofing>

Thank you!

Q & A

{skw17, wang-ch19}@mails.tsinghua.edu.cn