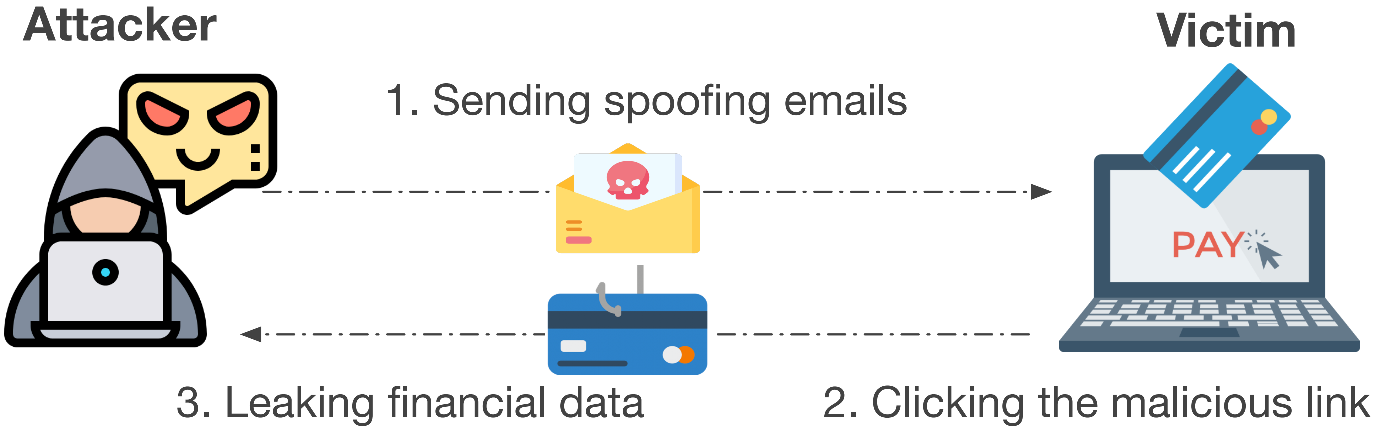
Weak Links in Authentication Chains:
A Large-scale Analysis of Email Sender Spoofing Attacks

Kaiwen Shen[1], Chuhan Wang[1], Minglei Guo, Xiaofeng Zheng, Chaoyi Lu,
Baojun Liu, Yuxuan Zhao, Shuang Hao, Haixin Duan, Qingfeng Pan, Min Yang

Email: skw17@mails.tsinghua.edu.cn

Email Spoofing Attacks

❖ How Email Spoofing Attacks Happen:



Attacker

Victim

1. Sending spoofing emails

2. Clicking the malicious link

3. Leaking financial data

❖ Impact of Email Spoofing Attack Today

600%

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

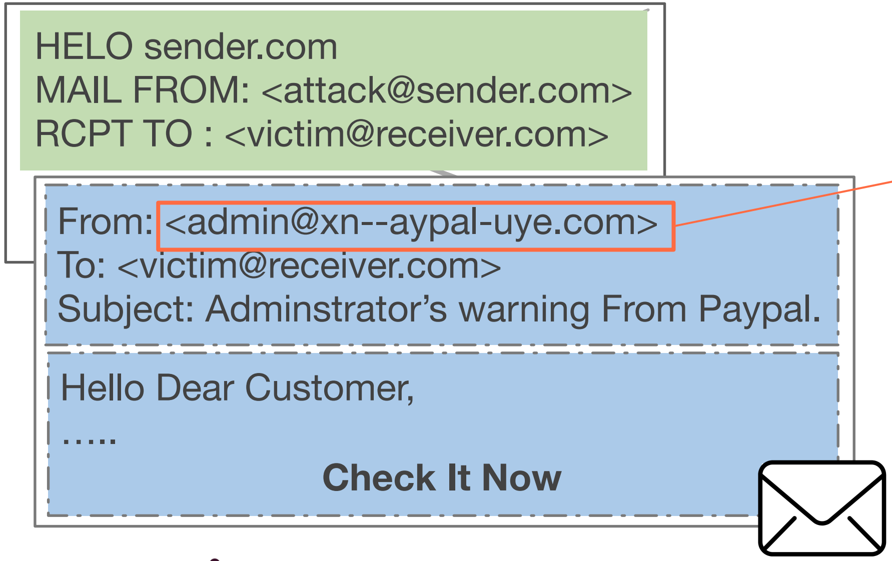
> ***"The most devastating attacks by the most sophisticated attackers, almost always begin with the simple act of spearphishing." Jeh Johnson Former Secretary, Department of Homeland Security***

$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>
```

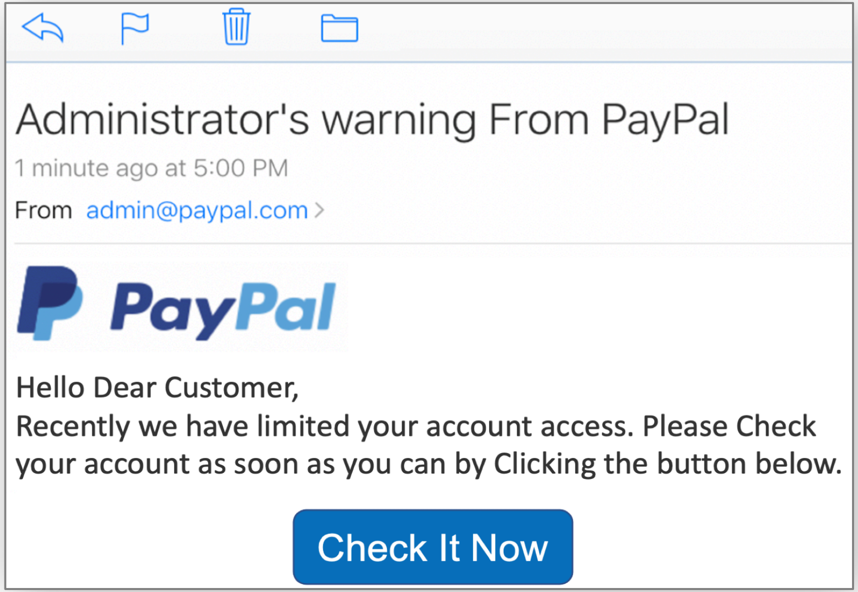
```
From: <admin@xn--aypal-uye.com>
To: <victim@receiver.com>
Subject: Adminstrator’s warning From Paypal.
```

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.

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

It’s so hard to spot spoofing email !

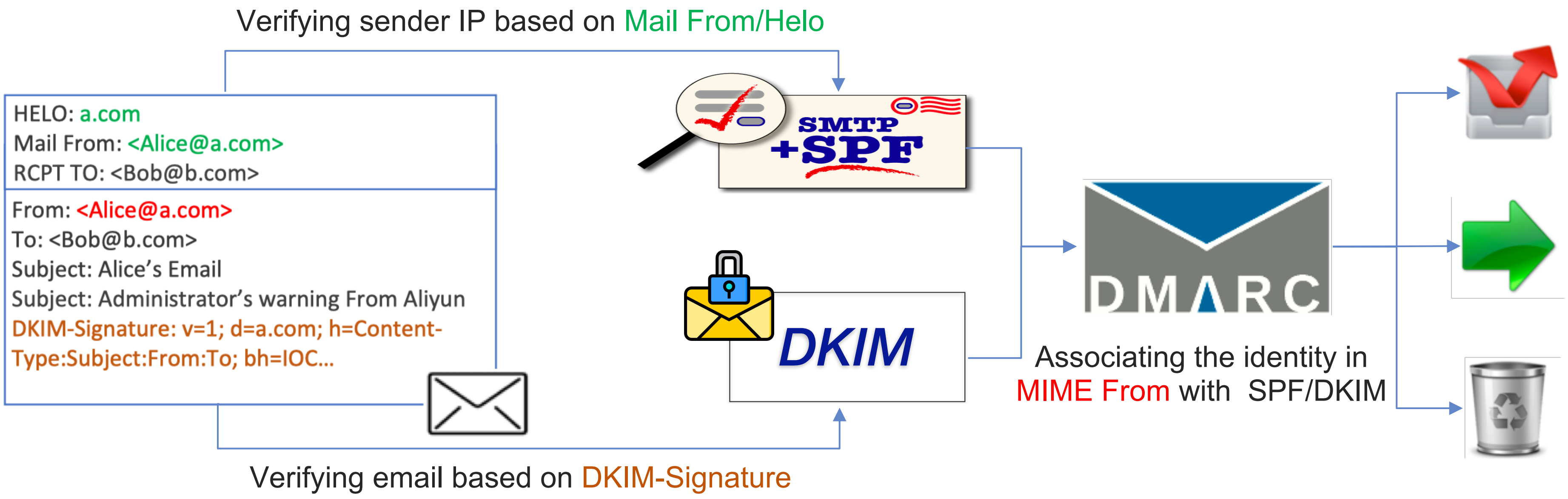
Email Spoofing Protections

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:



Verifying sender IP based on Mail From/Helo

HELO: a.com
Mail From: <Alice@a.com>
RCPT TO: <Bob@b.com>

From: <Alice@a.com>
To: <Bob@b.com>
Subject: Alice's Email
Subject: Administrator's warning From Aliyun
DKIM-Signature: v=1; d=a.com; h=Content-Type:Subject:From:To; bh=IOC...

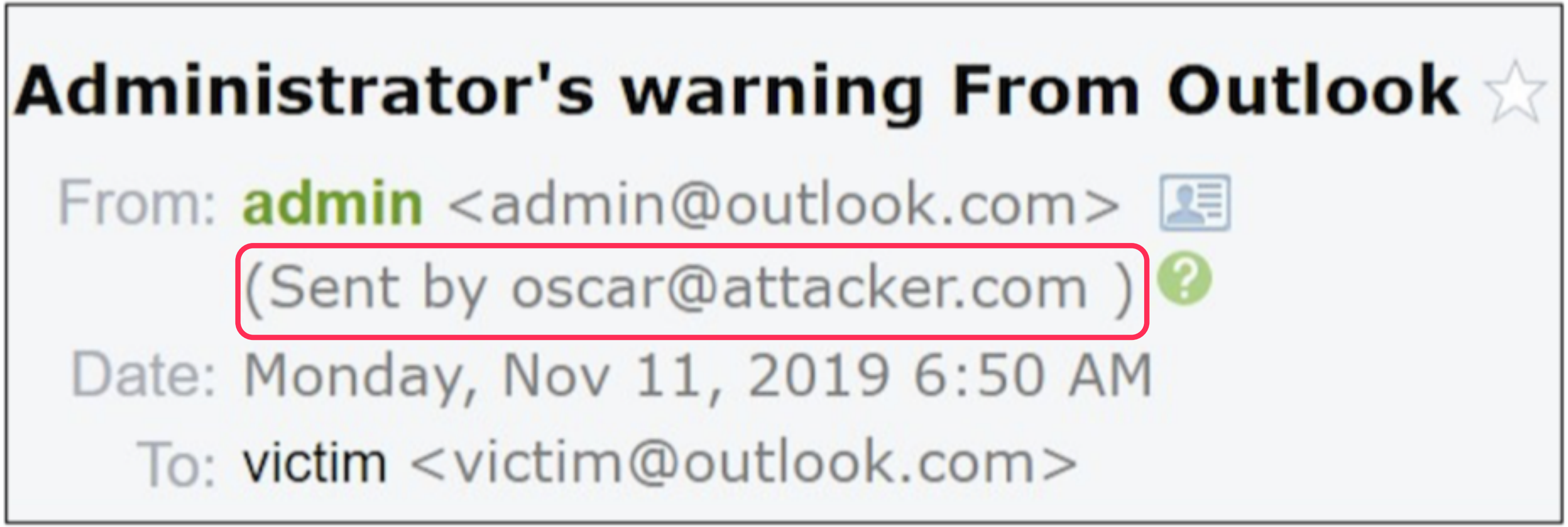
Verifying email based on DKIM-Signature

Associating the identity in MIME From with SPF/DKIM

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>

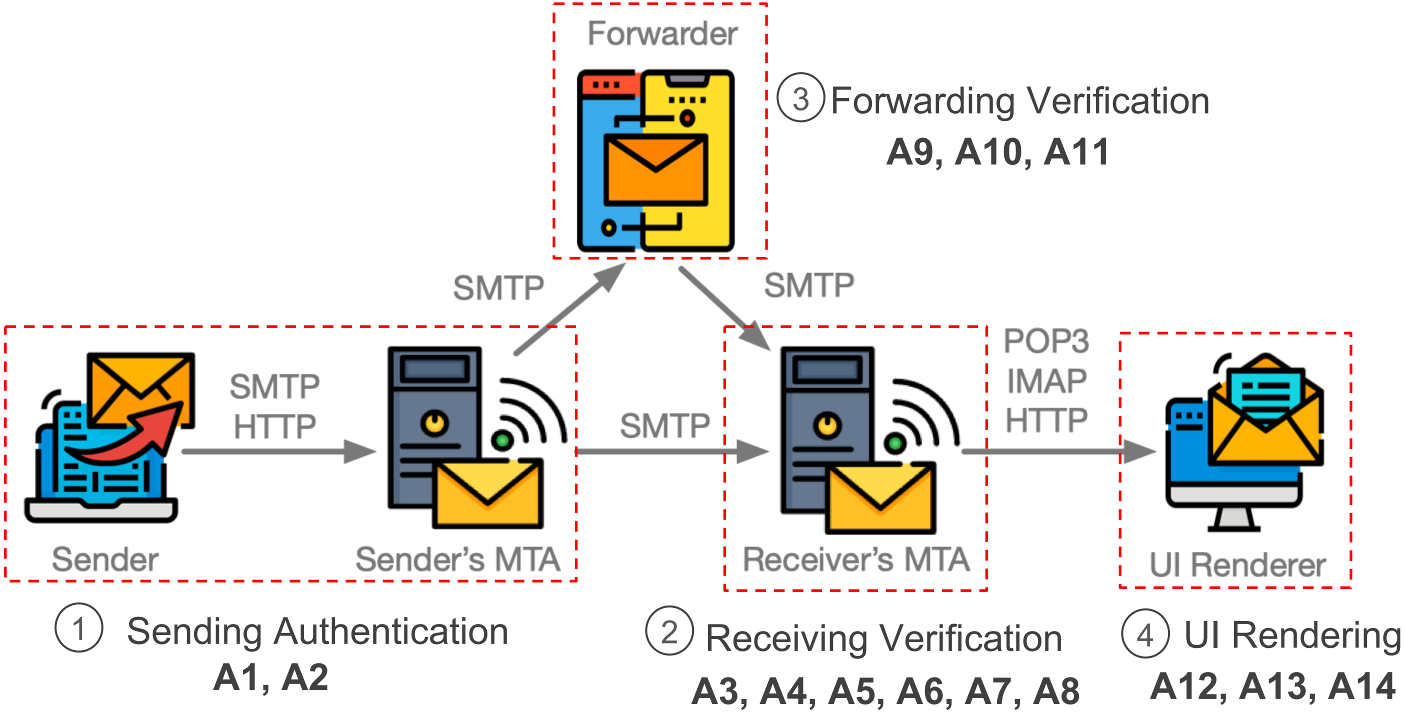
A spoofing email that fails the Sender Inconsistency Checks.

With these anti-spoofing protections,

why email spoofing attack is still possible ?

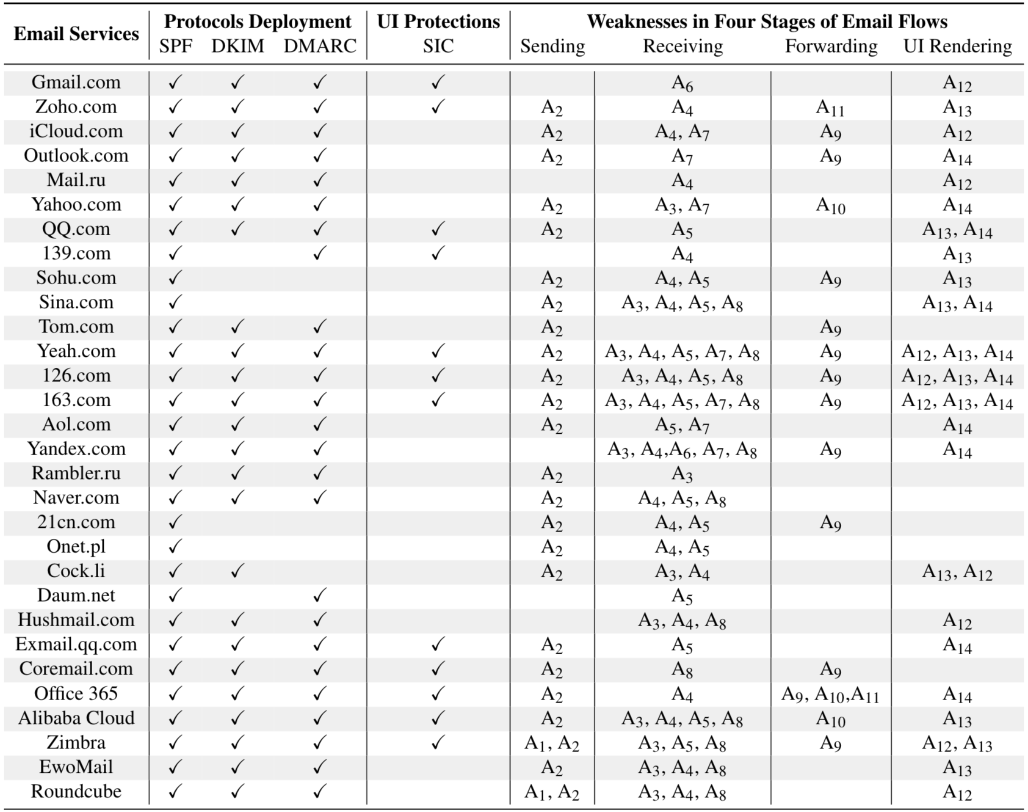
Our Works

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

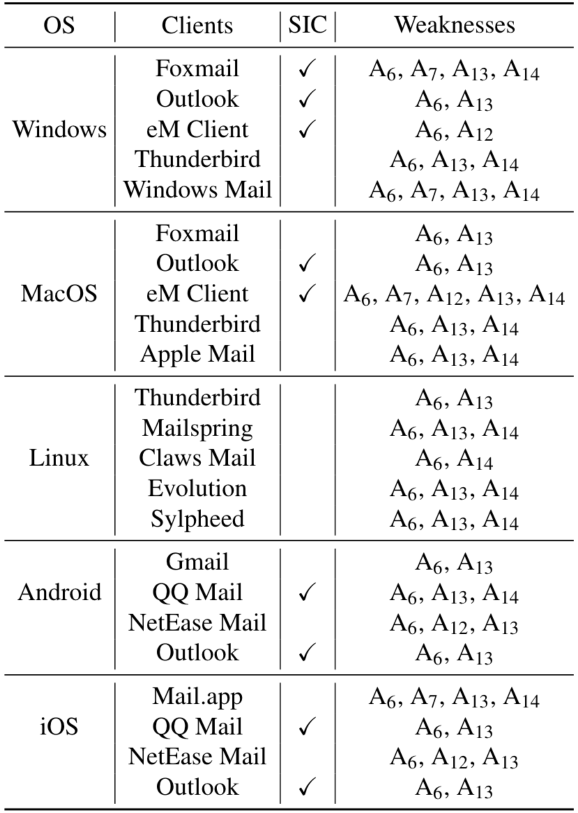


Measurement and Evaluation in the Real-world

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



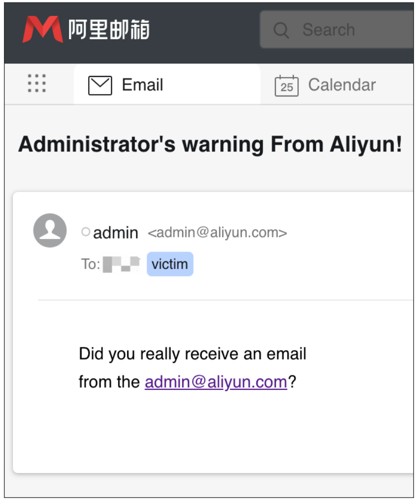
Email Services	Protocols Deployment			UI Protections	Weaknesses in Four Stages of Email Flows			
	SPF	DKIM	DMARC	SIC	Sending	Receiving	Forwarding	UI Rendering
Gmail.com	✓	✓	✓	✓		A_6		A_{12}
Zoho.com	✓	✓	✓	✓	A_2	A_4	A_{11}	A_{13}
iCloud.com	✓	✓	✓		A_2	A_4, A_7	A_9	A_{12}
Outlook.com	✓	✓	✓		A_2	A_7	A_9	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}
	Windows Mail		A_6, A_7, A_{13}, A_{14}
MacOS	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}
	Apple Mail		A_6, A_{13}, A_{14}
Linux	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}
	Sylpheed		A_6, A_{13}, A_{14}
Android	Gmail		A_6, A_{13}
	QQ Mail	✓	A_6, A_{13}, A_{14}
	NetEase Mail		A_6, A_{12}, A_{13}
	Outlook	✓	A_6, A_{13}
iOS	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 Real-world

Gmail
YAHOO! MAIL
163 网易免费邮 mail.163.com
Coremail 邮件系统专家 沟通创造价值
Outlook
Yandex Mail
QQ邮箱 mail.qq.com
FOXMAIL
mail.ru group
Apple Mail
阿里邮箱

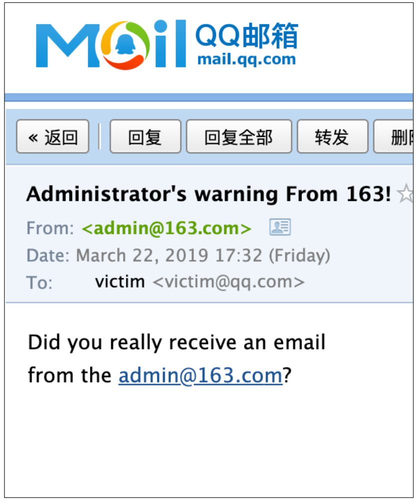


Administrator's warning From Aliyun!

admin <admin@aliyun.com>

To: victim

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



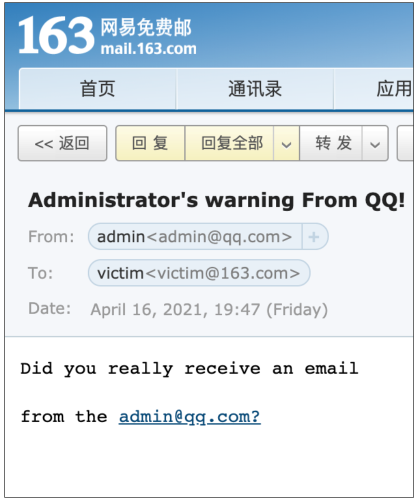
Administrator's warning From 163!

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?



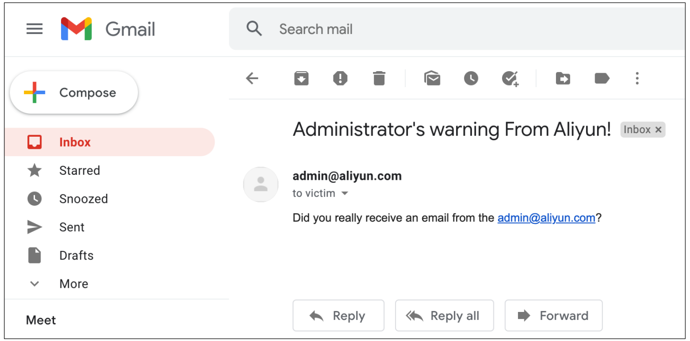
Administrator's warning From QQ!

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?

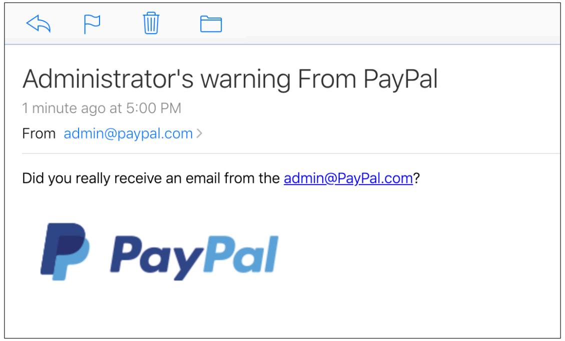


Administrator's warning From Aliyun! Inbox ×

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?

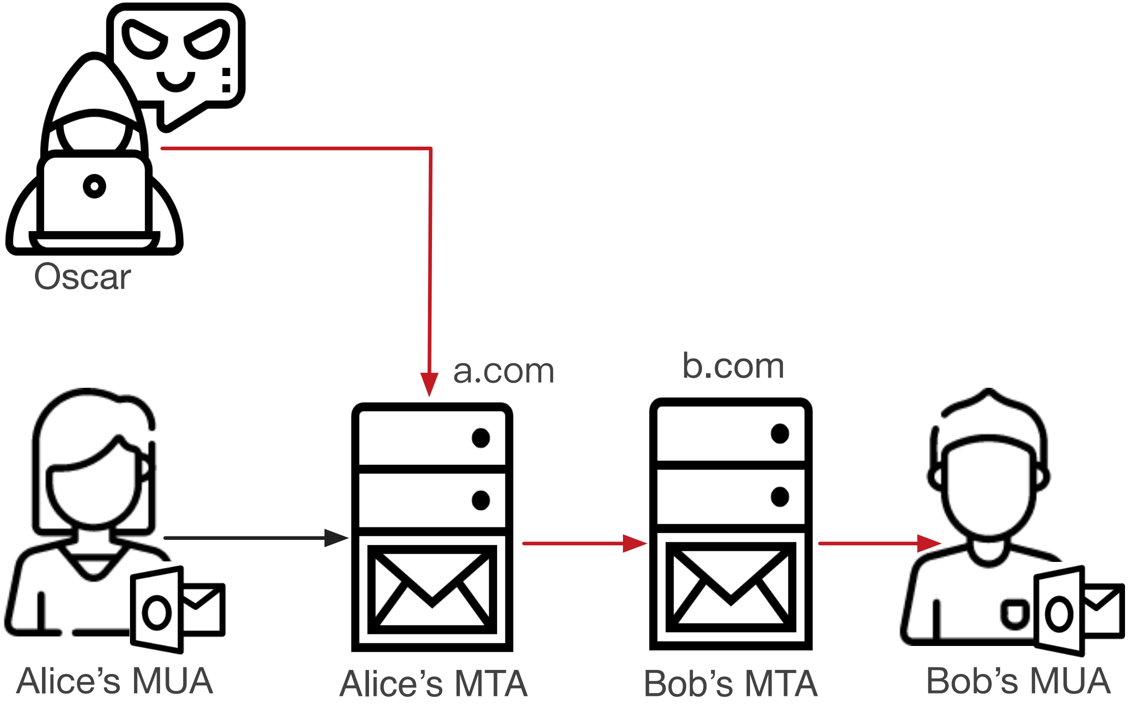
All of tested email services are vulnerable to certain types of attacks.

Attacks

Three Types of Attack Models

a. Shared MTA Attack

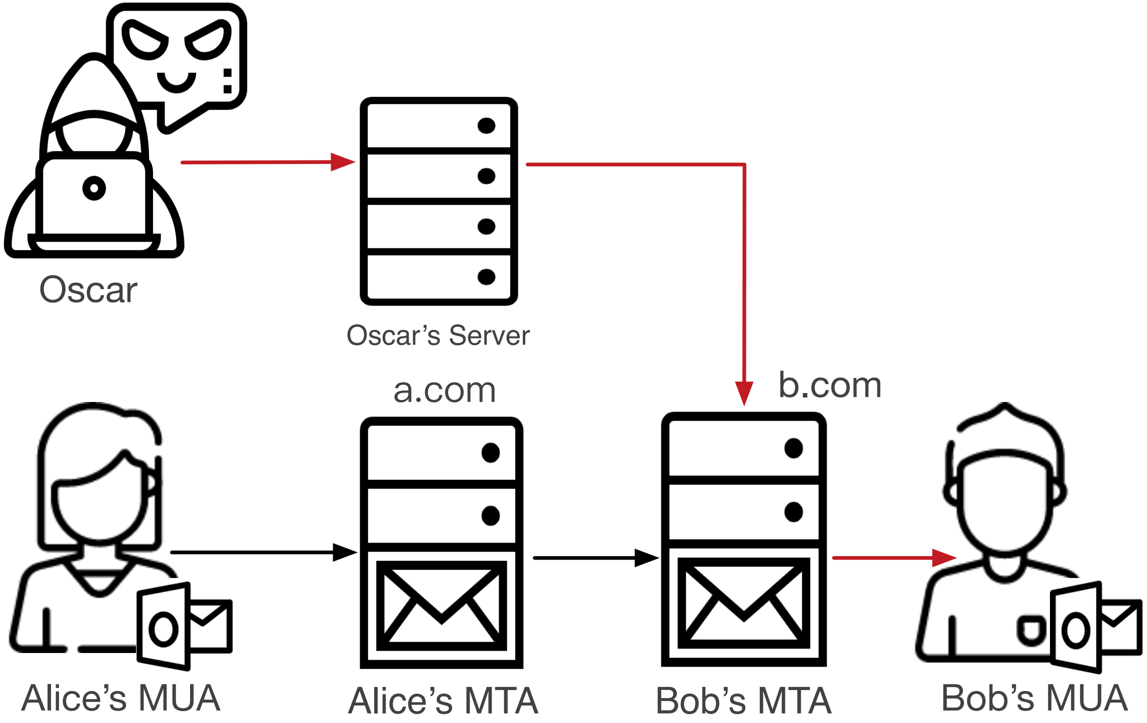
Oscar@a.com sends spoofing email as Alice@a.com with the a.com MTA



Three Types of Attack Models

b. Direct MTA Attack

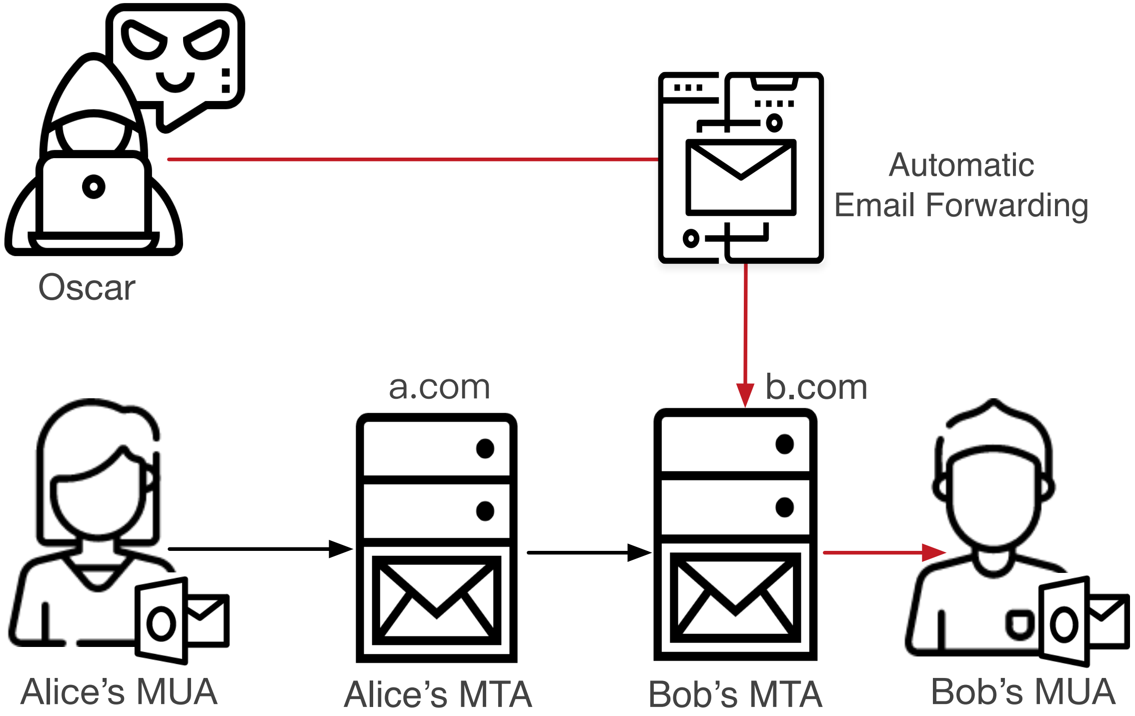
Oscar sends spoofing email through his self-build email server.



Three Types of Attack Models

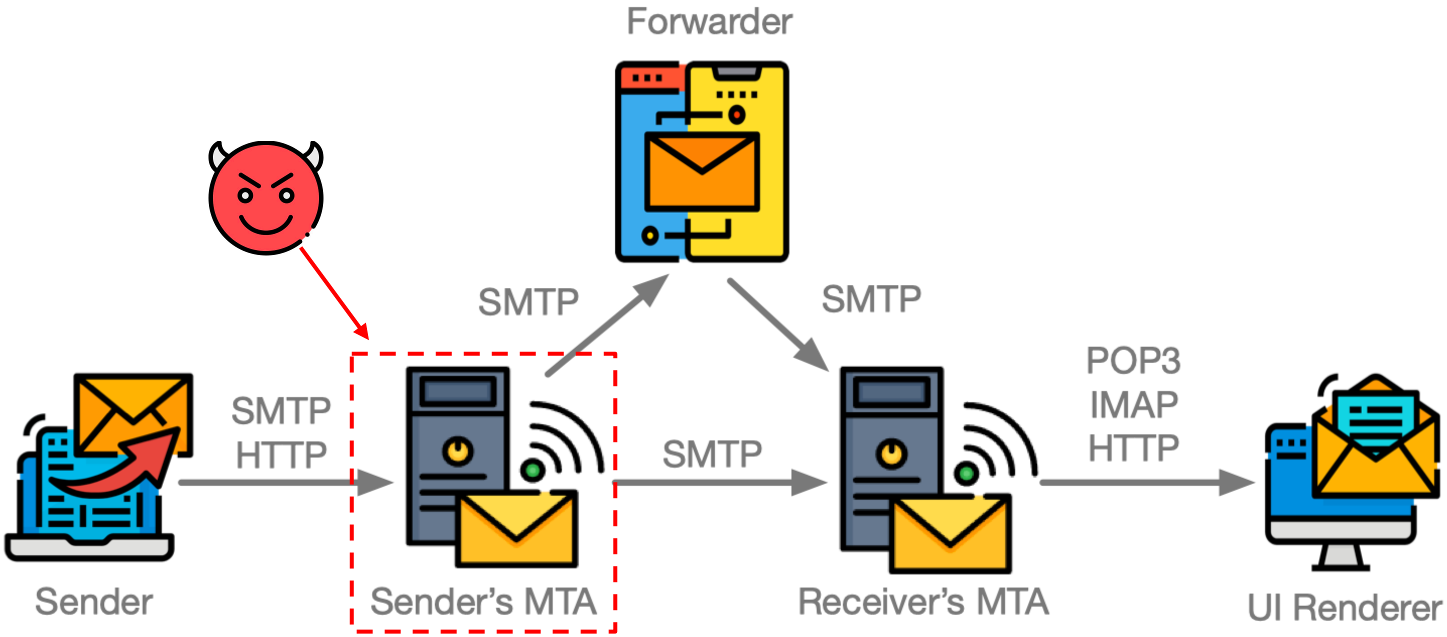
c. Forward MTA Attack

Oscar abuses email forwarding service to send spoofing emails.



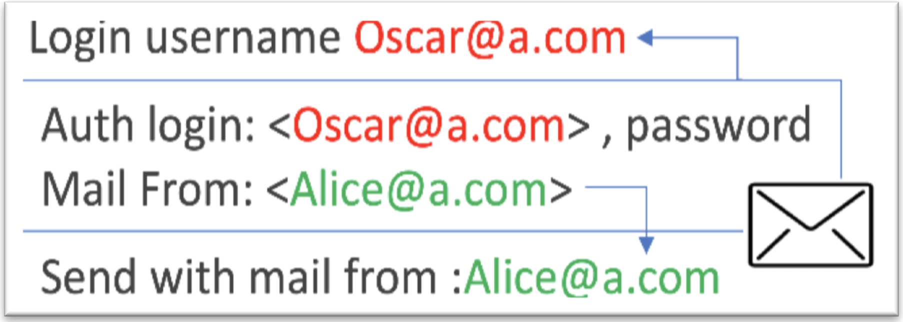
Attacks in Email Sending Authentication

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



Attacks in Email Sending Authentication

- **Auth Username ≠ Mail From (A1)**



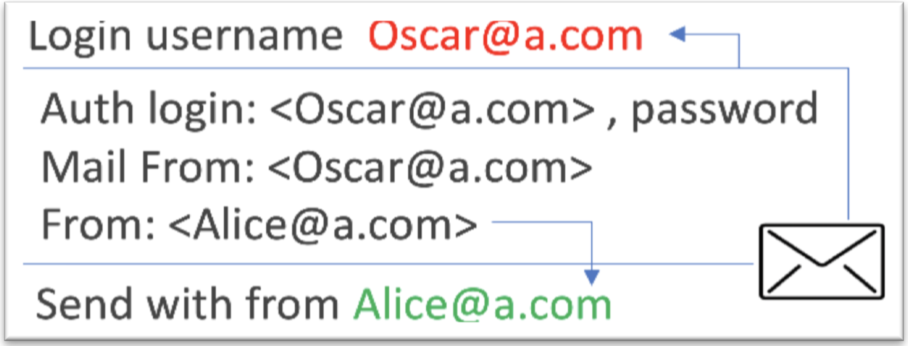
Login username Oscar@a.com

Auth login: <Oscar@a.com> , password

Mail From: <Alice@a.com>

Send with mail from :Alice@a.com

- **Mail From ≠ From (A2)**



Login username Oscar@a.com

Auth login: <Oscar@a.com> , password

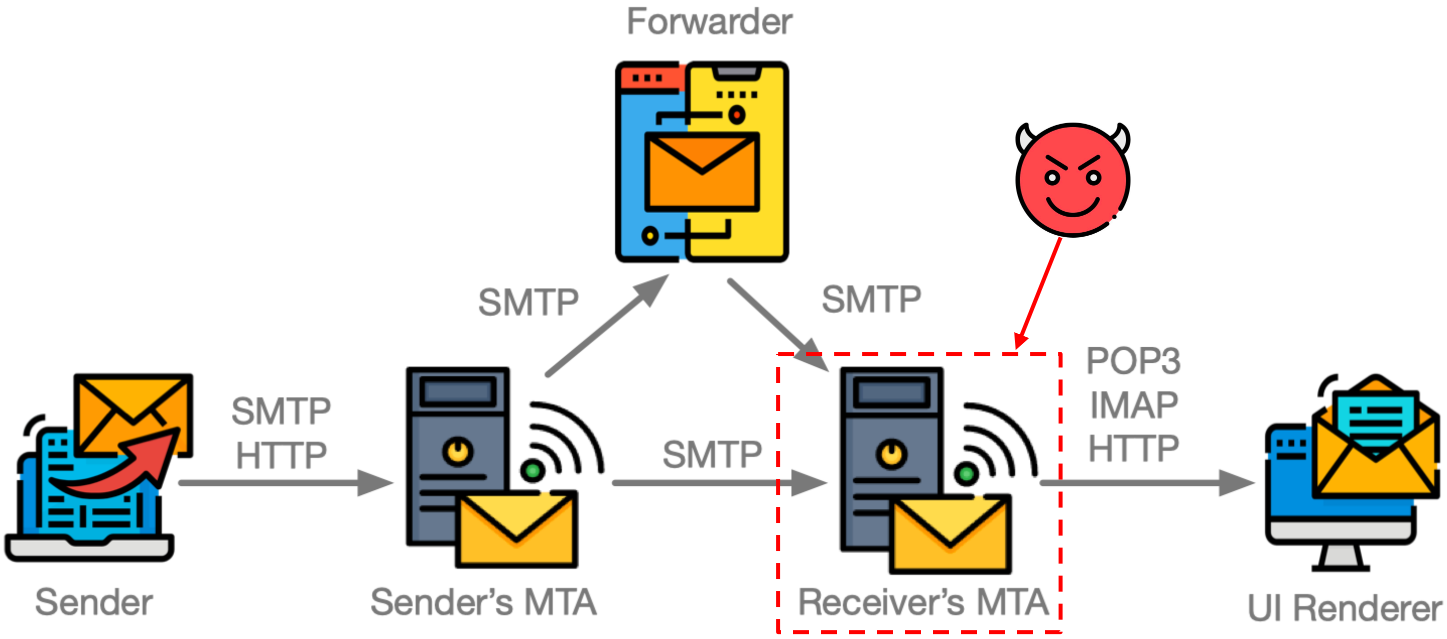
Mail From: <Oscar@a.com>

From: <Alice@a.com>

Send with from Alice@a.com

Attacks in Email Receiving Verification

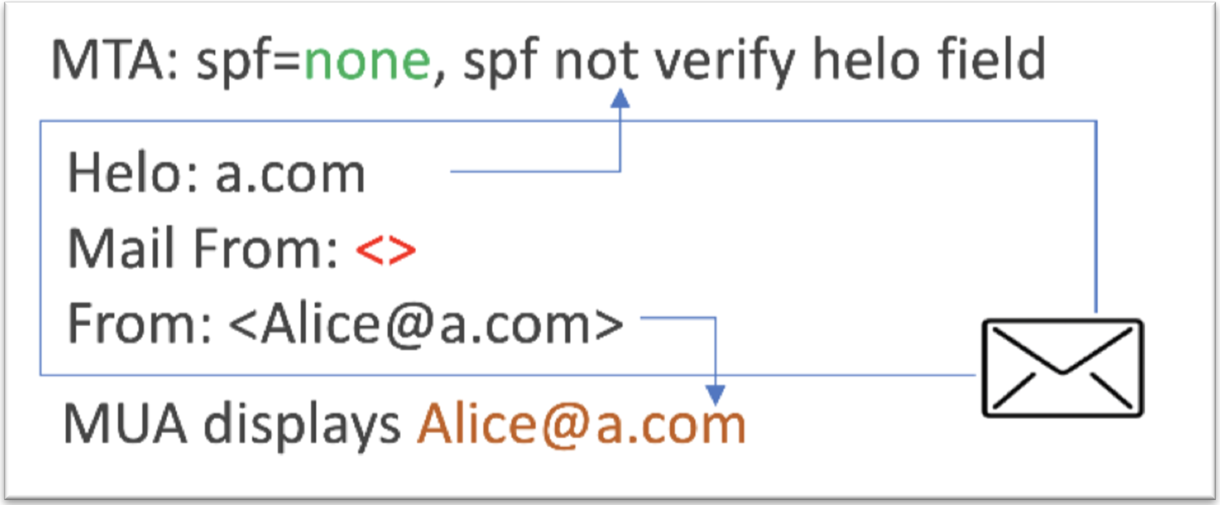
- **Successful Attacks:** bypassing SPF, DKIM and DMARC.
- **Benefits:** hard to spot spoofing email passing three security protocols.



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



MTA: spf=none, spf not verify helo field

Helo: a.com

Mail From: <>

From: <Alice@a.com>

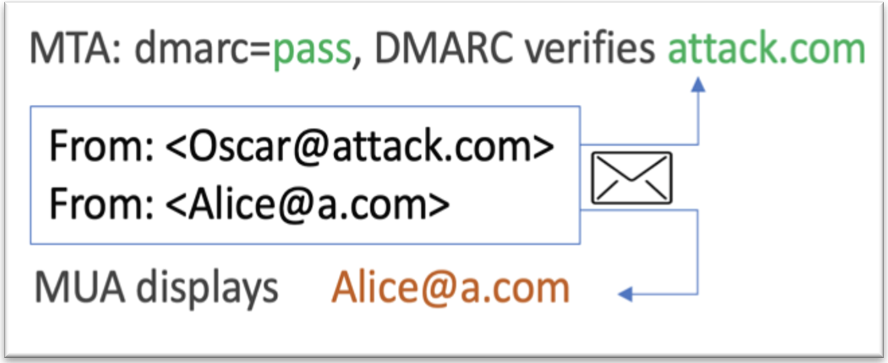
MUA displays Alice@a.com

Empty Mail From attack bypassing the SPF verification

Attacks in Email Receiving Verification

Inconsistent Parsing of Ambiguous Emails

- Multiple from headers(A4)

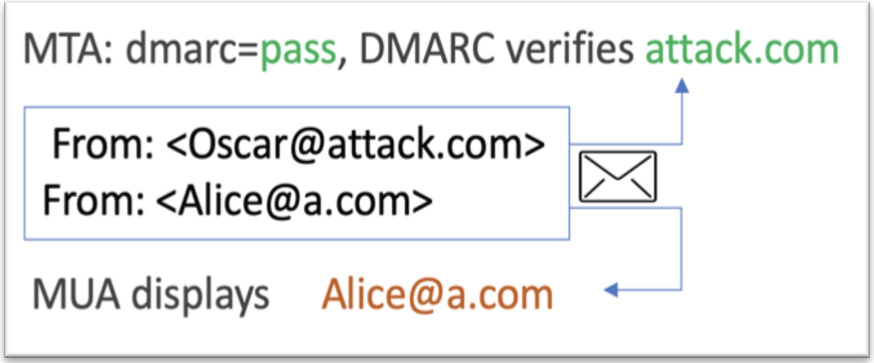


MTA: dmarc=pass, DMARC verifies attack.com

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

MUA displays Alice@a.com

Ordinary multiple From attack



MTA: dmarc=pass, DMARC verifies attack.com

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

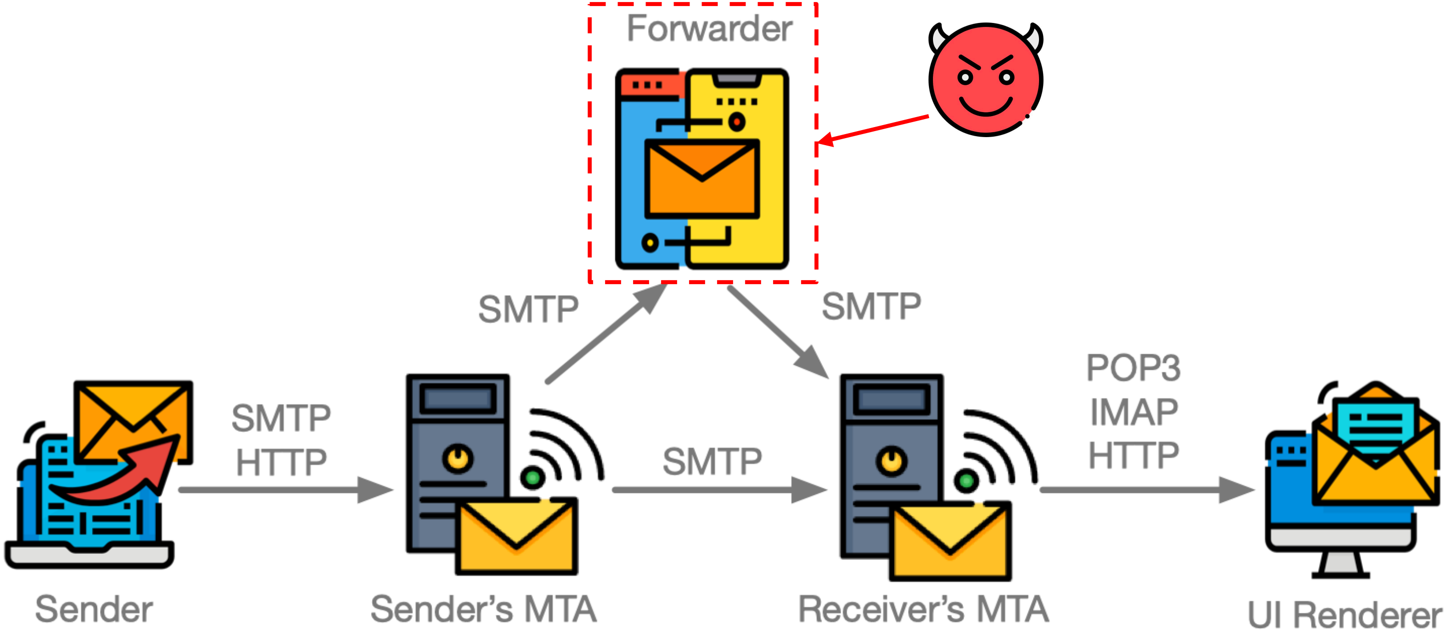
MUA displays Alice@a.com

Multiple From attack with spaces

Attacks in Email Forwarding Verification

Successful Attacks:

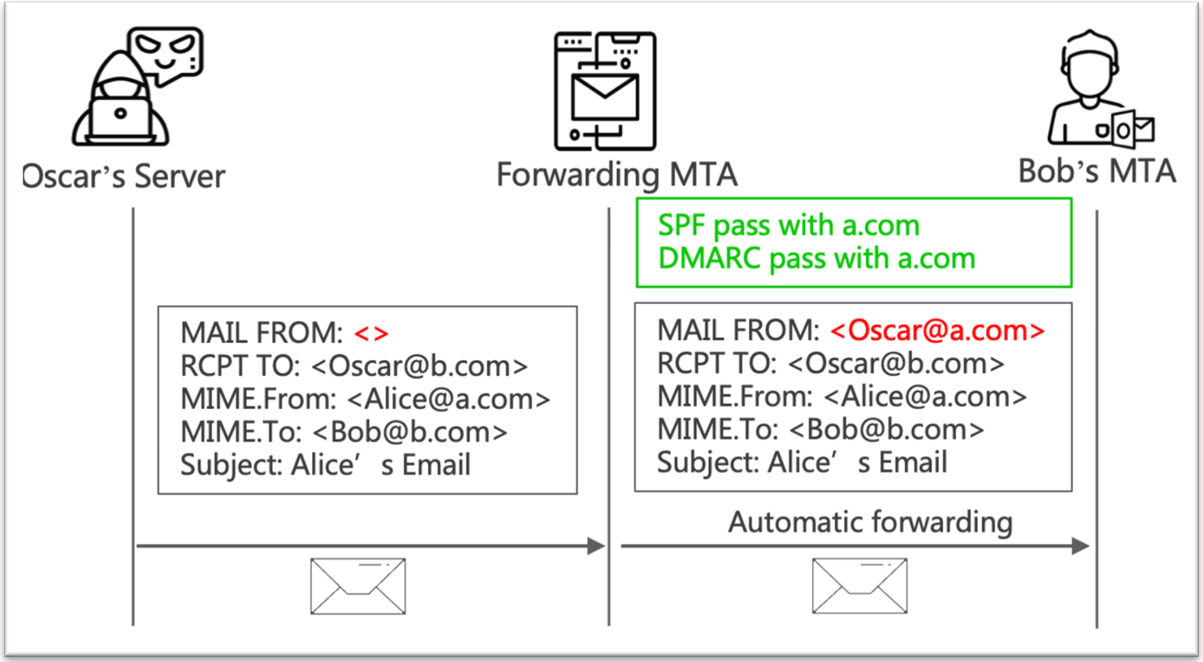
- Freely configure without authentication verification
- A higher security endorsement



Attacks in Email Forwarding Verification

Unauthorized Forwarding Attack (A9)

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



SPF pass with a.com
DMARC pass with a.com

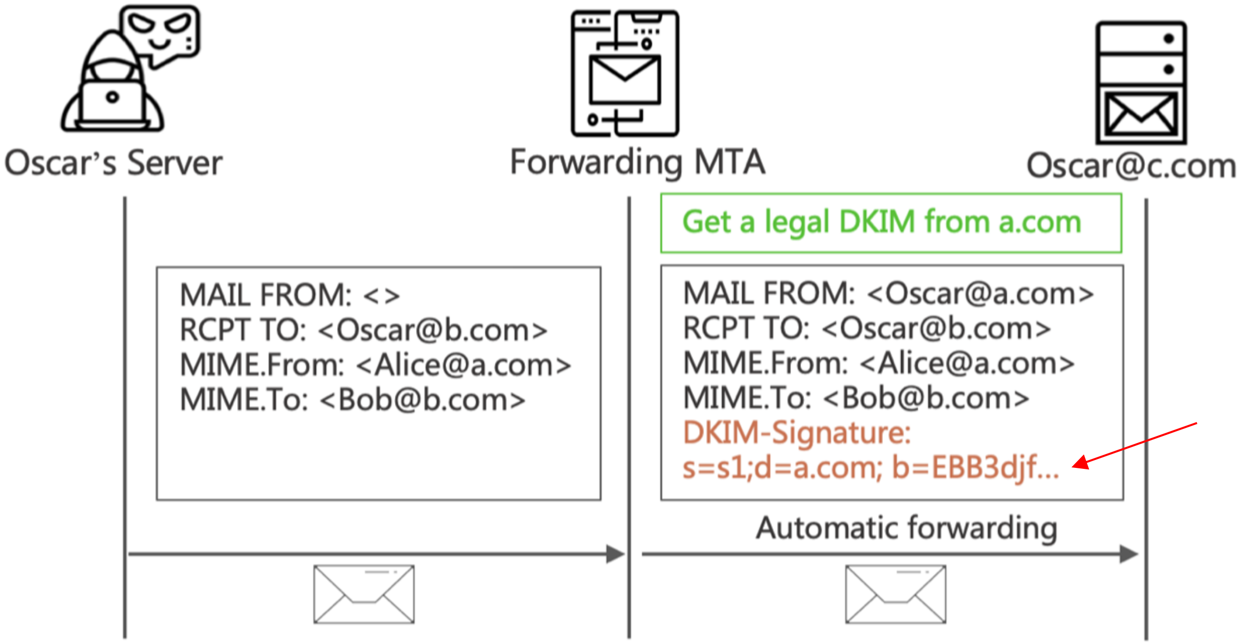
MAIL FROM: <>
RCPT TO: <Oscar@b.com>
MIME.From: <Alice@a.com>
MIME.To: <Bob@b.com>
Subject: Alice’ s Email

MAIL FROM: <Oscar@a.com>
RCPT TO: <Oscar@b.com>
MIME.From: <Alice@a.com>
MIME.To: <Bob@b.com>
Subject: Alice’ s Email

Attacks in Email Forwarding Verification

DKIM-Signature Fraud Attack (A10)

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



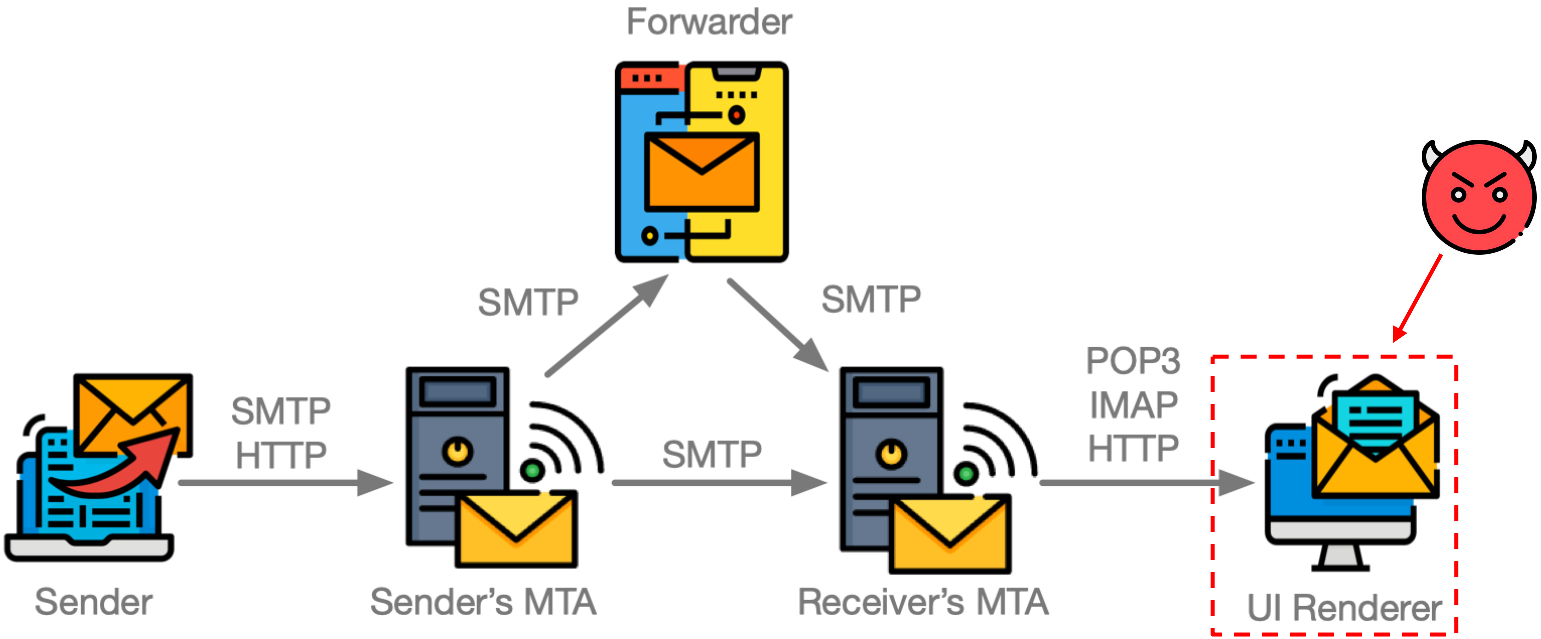
MAIL FROM: <>
RCPT TO: <Oscar@b.com>
MIME.From: <Alice@a.com>
MIME.To: <Bob@b.com>

MAIL FROM: <Oscar@a.com>
RCPT TO: <Oscar@b.com>
MIME.From: <Alice@a.com>
MIME.To: <Bob@b.com>
DKIM-Signature:
s=s1;d=a.com; b=EBB3djf...

Attacks in Email UI Rendering

Successful Attack:

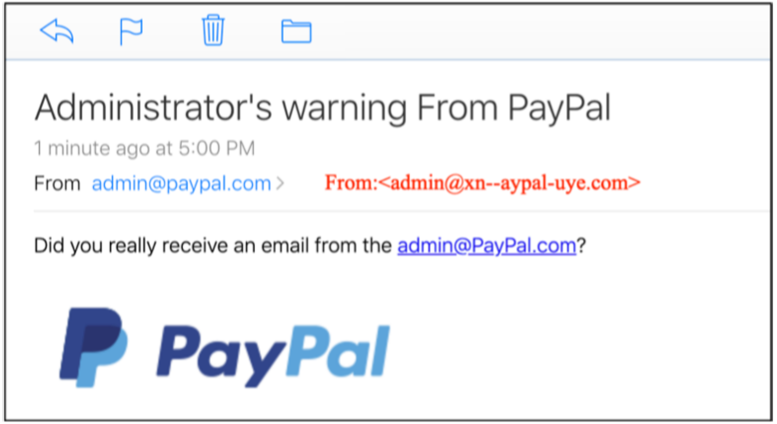
- ❖ The displayed address is inconsistent with the real one.
- ❖ No any security alerts on the MUA.



Attacks in Email UI Rendering

New Challenge : International Email

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



Administrator's warning From PayPal

1 minute ago at 5:00 PM

From admin@paypal.com >   From:<admin@xn--aypal-uye.com>

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

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)

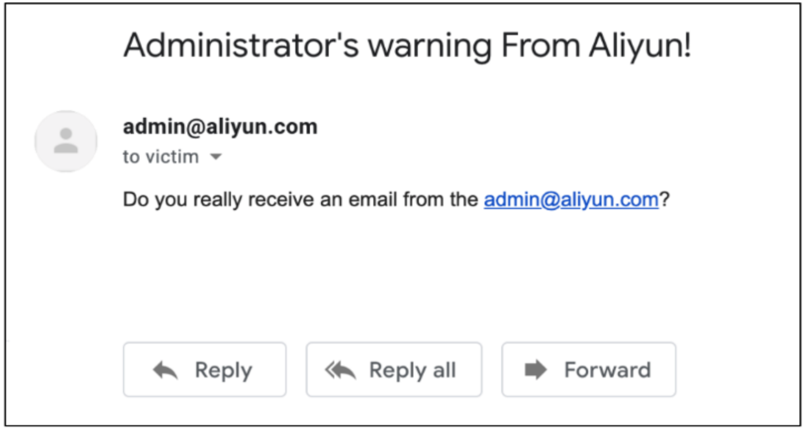
Combined Attack

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 Attacks:

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

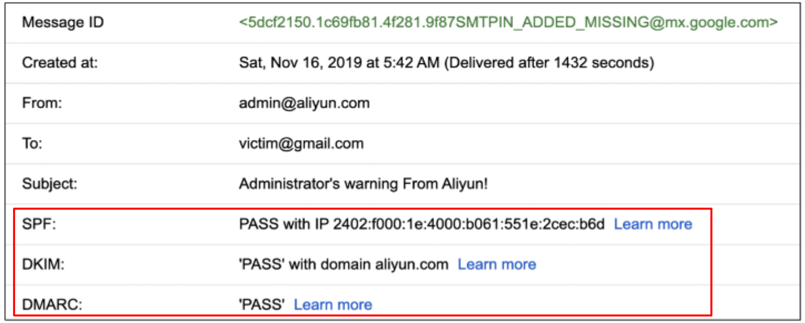


Administrator's warning From Aliyun!

admin@aliyun.com
to victim

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

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



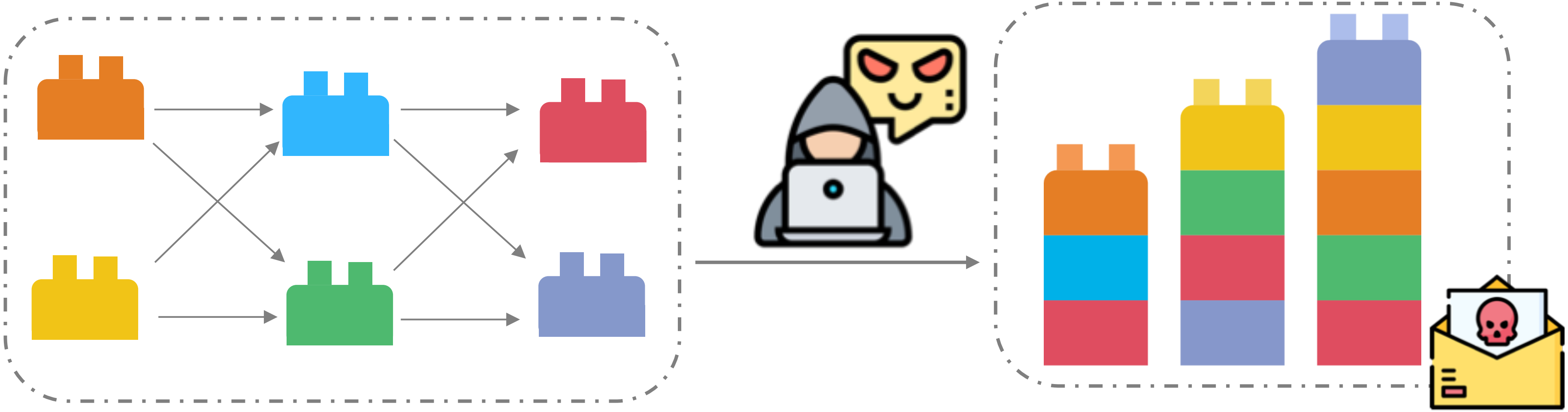
Message ID	<5dcf2150.1c69fb81.4f281.9f87SMTPIN_ADDED_MISSING@mx.google.com>
Created at:	Sat, Nov 16, 2019 at 5:42 AM (Delivered after 1432 seconds)
From:	admin@aliyun.com
To:	victim@gmail.com
Subject:	Administrator's warning From Aliyun!
SPF:	PASS with IP 2402:f000:1e:4000:b061:551e:2cec:b6d Learn more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

Combined Attacks

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



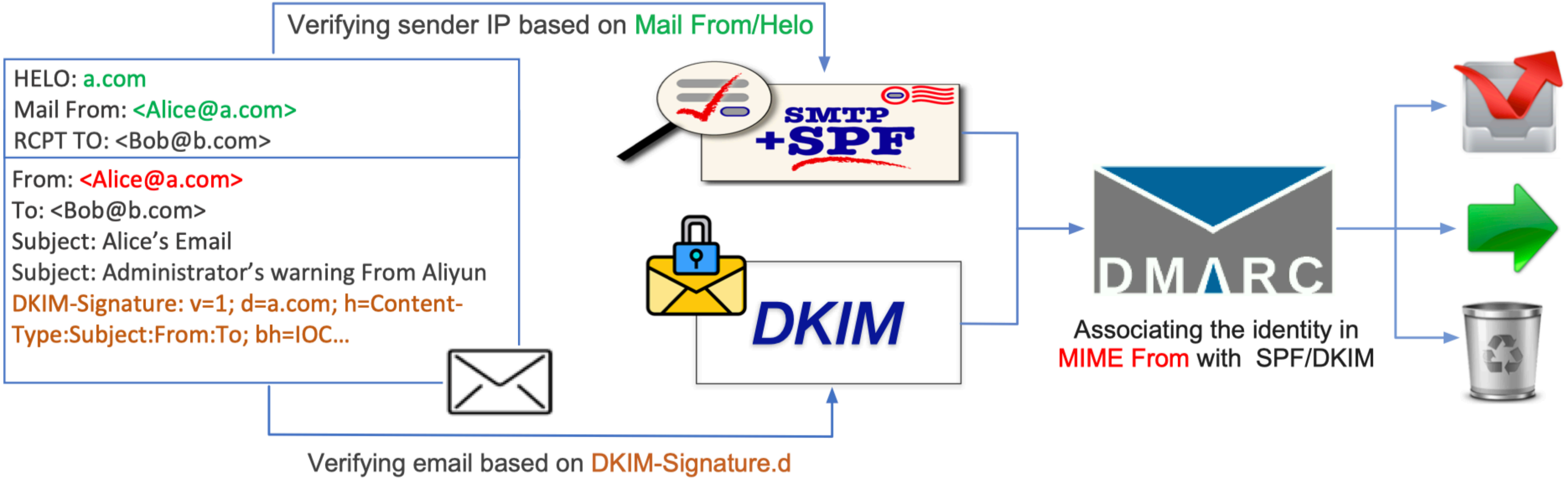
Different Attack Models/Techniques

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.



Verifying sender IP based on Mail From/Helo

HELO: a.com
Mail From: <Alice@a.com>
RCPT TO: <Bob@b.com>

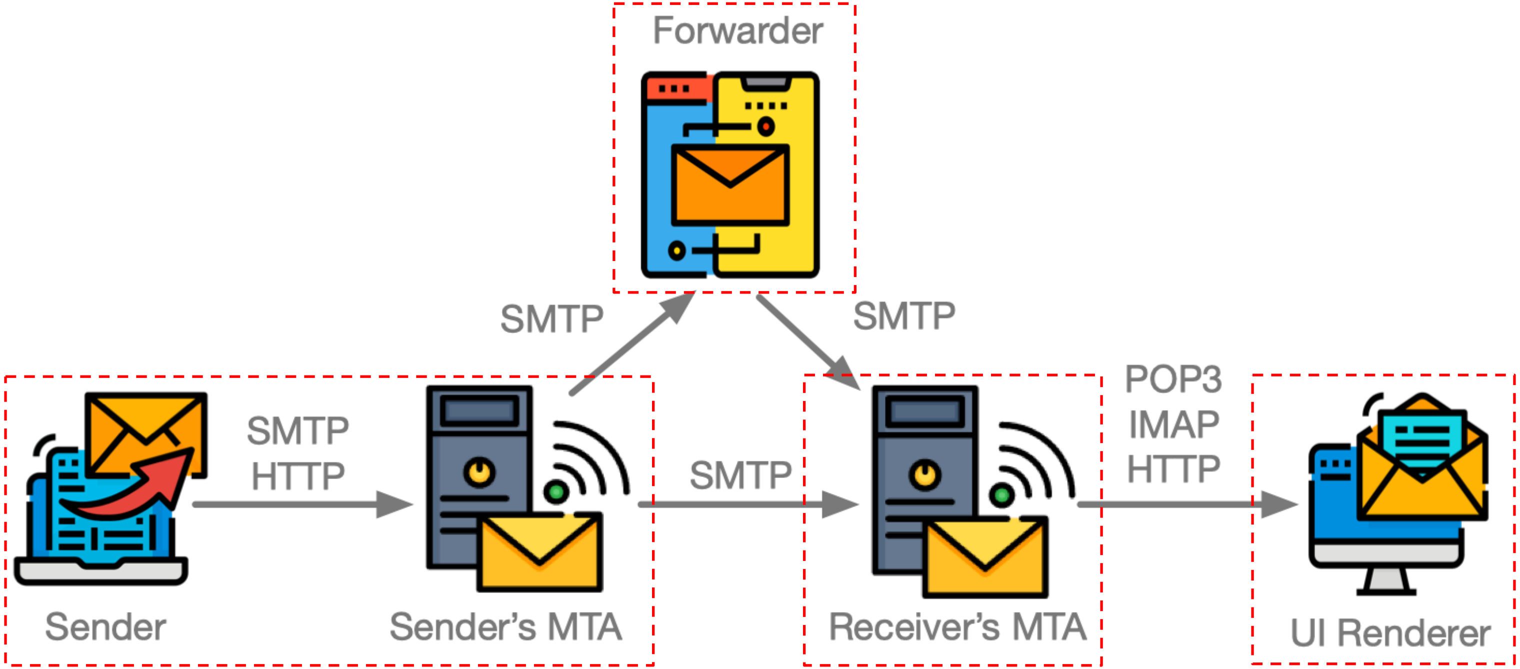
From: <Alice@a.com>
To: <Bob@b.com>
Subject: Alice’s Email
Subject: Administrator’s warning From Aliyun
DKIM-Signature: v=1; d=a.com; h=Content-Type:Subject:From:To; bh=IOC...

Associating the identity in MIME From with SPF/DKIM

Verifying email based on DKIM-Signature.d

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.

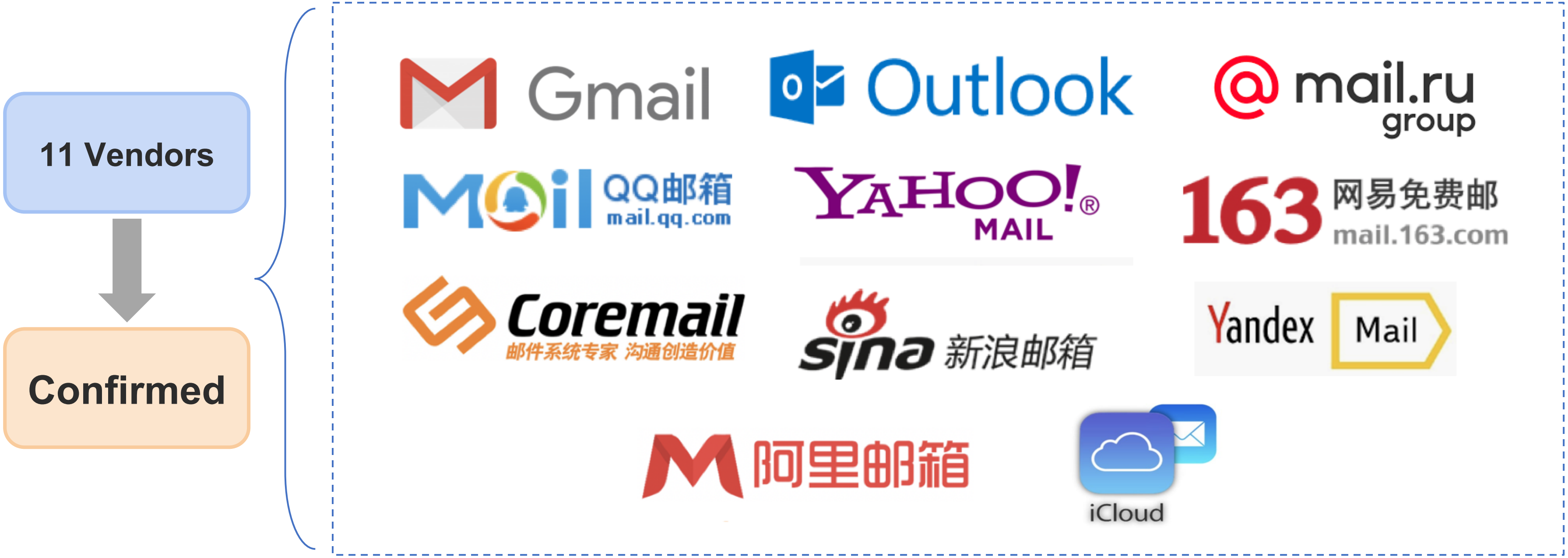
Mail QQ邮箱 mail.qq.com
sina 新浪邮箱
163 网易免费邮 mail.163.com
Coremail 邮件系统专家 沟通创造价值
阿里邮箱
搜狐闪电邮箱 mail.sohu.com
中国电信 CHINA TELECOM 189 邮箱
中国移动通信 CHINA MOBILE 139邮箱
Gmail
Outlook
YAHOO! MAIL
Yandex Mail
Thunderbird
FOXMAIL
iCloud
eM Client

The inconsistency among different services creates security threats.

Mitigation

Responsible Disclosure

- Helping email vendors mitigate identified email spoofing attacks.
  - Vendors have 10 months to mitigate it before this paper is published.



11 Vendors

Confirmed

Mitigation and Solution

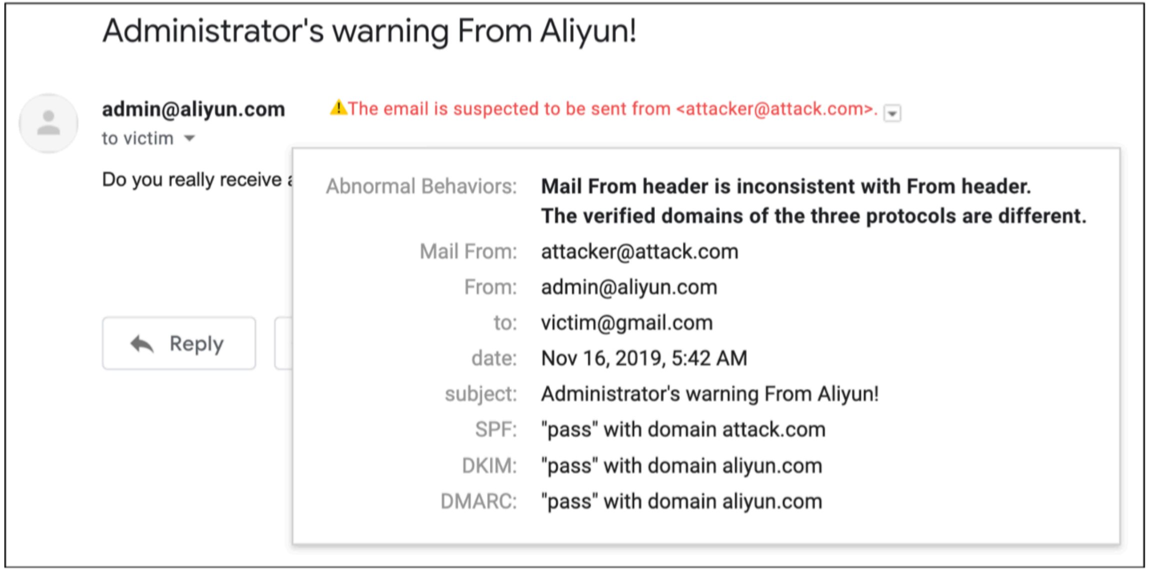
❖ UI Notification:

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

to victim ▾

Do you really receive a

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

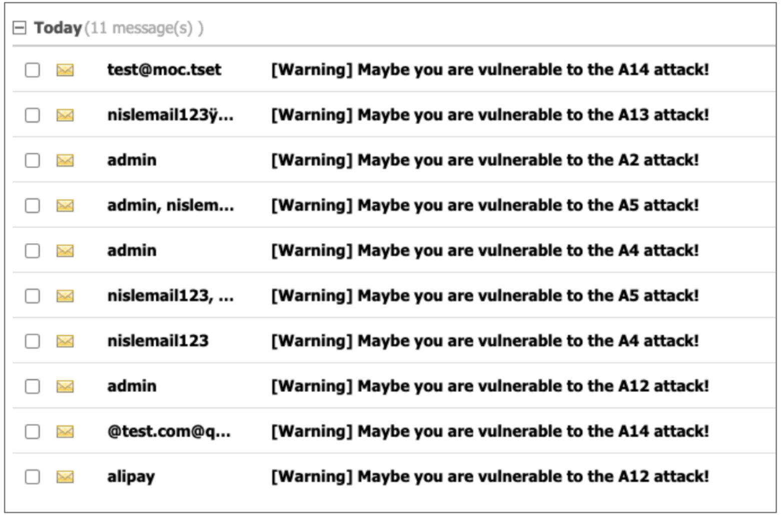
An example of UI notification against the combined attack

https://chrome.google.com/webstore/detail/nospoofing/ehidaopjcnapdglbbbjgeoagpophfjnp

Mitigation and Solution

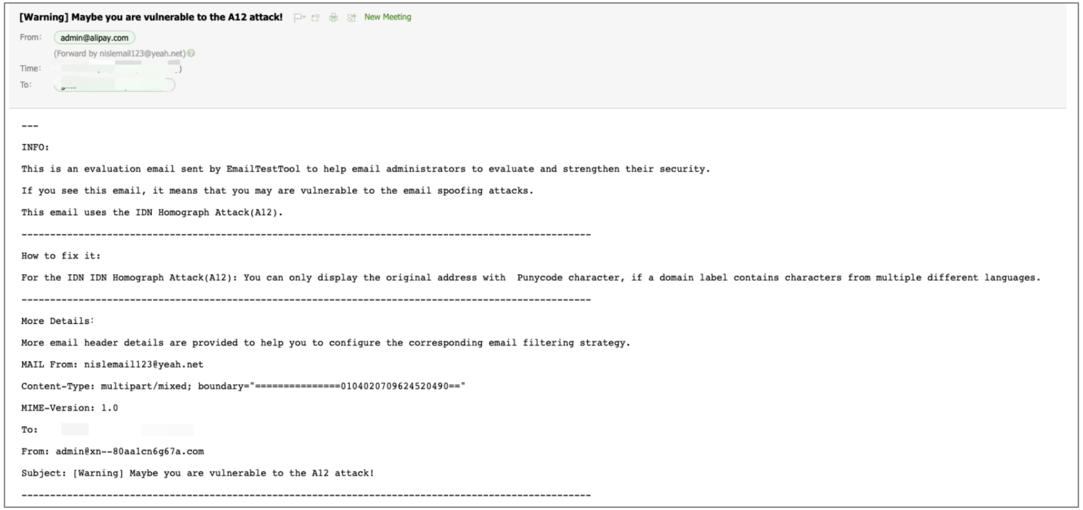
❖ Evaluation Tools:

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



⊟ **Today** (11 message(s))

□	✉	**test@moc.tset**	**[Warning] Maybe you are vulnerable to the A14 attack!**
□	✉	**nislemail123ÿ...**	**[Warning] Maybe you are vulnerable to the A13 attack!**
□	✉	**admin**	**[Warning] Maybe you are vulnerable to the A2 attack!**
□	✉	**admin, nislem...**	**[Warning] Maybe you are vulnerable to the A5 attack!**
□	✉	**admin**	**[Warning] Maybe you are vulnerable to the A4 attack!**
□	✉	**nislemail123, ...**	**[Warning] Maybe you are vulnerable to the A5 attack!**
□	✉	**nislemail123**	**[Warning] Maybe you are vulnerable to the A4 attack!**
□	✉	**admin**	**[Warning] Maybe you are vulnerable to the A12 attack!**
□	✉	**@test.com@q...**	**[Warning] Maybe you are vulnerable to the A14 attack!**
□	✉	**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: [redacted])
To: [redacted]

```
---

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 are 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: [redacted]

From: admin@xn--80aalcn6g67a.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