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
Email Spoofing Attacks

How Email Spoofing Attacks Happen:

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: Administrator's warning From Paypal.

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:

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

DKIM

Associating the identity in MIME From with SPF/DKIM

DMARC
Email Spoofing Protections

UI-level Spoofing Protection

- Sender Inconsistency Checks (SIC)

A spoofing email that fails the Sender Inconsistency Checks.
With these anti-spoofing protections, why email spoofing attack is still possible?
Our Work

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

![Diagram showing four stages of authentication: Sending Authentication (A1, A2), Receiving Verification (A3, A4, A5, A6, A7, A8), Forwarding Verification (A9, A10, A11), UI Rendering (A12, A13, A14).]
Measurement and Evaluation in the Wild

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

<table>
<thead>
<tr>
<th>Email Services</th>
<th>Protocols Deployment</th>
<th>UI Protections</th>
<th>Weaknesses in Four Stages of Email Flows</th>
<th>OS</th>
<th>Clients</th>
<th>SIC</th>
<th>Weaknesses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gmail.com</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>A6, A7, A13, A14</td>
<td>Windows</td>
<td>Foxmail, Outlook, eM Client, Thunderbird, Windows Mail</td>
<td>✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>Zoho.com</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>A6, A13</td>
<td>✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>iCloud.com</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>A6, A12</td>
<td>✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Outlook.com</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>A6, A13, A14</td>
<td>✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mail.ru</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>A4, A12</td>
<td>✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yahoo.com</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>A3, A7, A10</td>
<td>✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>QQ.com</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>A6, A13, A14</td>
<td>✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>139.com</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>A13, A14</td>
<td>✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sohu.com</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>A6, A7, A13, A14</td>
<td>✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sina.com</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>A6, A13, A14</td>
<td>✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tom.com</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>A6, A12</td>
<td>✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yeah.com</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>A6, A12, A13, A14</td>
<td>✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>126.com</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>A6, A12, A13, A14</td>
<td>✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>163.com</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>A6, A12, A13, A14</td>
<td>✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Aol.com</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>A6, A12, A13, A14</td>
<td>✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yandex.com</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>A6, A12, A13, A14</td>
<td>✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rambler.ru</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>A6, A12, A13, A14</td>
<td>✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Naver.com</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>A6, A12, A13, A14</td>
<td>✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>21cn.com</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>A6, A12, A13, A14</td>
<td>✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Onet.pl</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>A6, A12, A13, A14</td>
<td>✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cock.li</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>A6, A12, A13, A14</td>
<td>✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Daum.net</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>A6, A12, A13, A14</td>
<td>✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hushmail.com</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>A6, A12, A13, A14</td>
<td>✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exmail.qq.com</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>A6, A12, A13, A14</td>
<td>✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Coremail.com</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>A6, A12, A13, A14</td>
<td>✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Office 365</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>A6, A12, A13, A14</td>
<td>✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alibaba Cloud</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>A6, A12, A13, A14</td>
<td>✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Zimbra</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>A6, A12, A13, A14</td>
<td>✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EwoMail</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>A6, A12, A13, A14</td>
<td>✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Roundcube</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>A6, A12, A13, A14</td>
<td>✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Measurement and Evaluation in the Wild

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)**
  
  ![Diagram of Auth Username ≠ Mail From (A1)]

- **Mail From ≠ From (A2)**
  
  ![Diagram of 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

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

Ordinary multiple From attack

MTA: dmarc=pass, DMARC verifies attack.com

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)

Missing UI Rendering Attack (A13)

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

(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.
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.

Confirmed 11 Vendors

- Gmail
- Outlook
- mail.ru
- QQ邮箱
- Yahoo Mail
- 163 网易免费邮
- Coremail
- sina 新浪邮箱
- Yandex Mail
- 阿里邮箱
- iCloud
Mitigation and Solution

❖ UI Notification:

NoSpoofing: a chrome extension for Gmail.

An example of UI notification against the combined attack

https://chrome.google.com/webstore/detail/nospoofing/ehidaopjcnapdglbblbijeoagpofhpjop
Mitigation and Solution

❖ Evaluation Tools:

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

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