身份验证链中的薄弱环节：对电子邮件发件人欺骗攻击的大规模分析

Kaiwen Shen, Chuhan Wang, and Minglei Guo, 清华大学; Xiaofeng Zheng, 清华大学和奇安信技术研究院; Chaoyi Lu 和 Baojun Liu, 清华大学; Yuxuan Zhao, 华北计算技术研究所; 郝爽, 德克萨斯大学达拉斯分校; 清华大学段海欣; 奇安信技术研究院; Qingfeng Pan, Coremail Technology Co. Ltd; 杨敏, 复旦大学

https://www.usenix.org/conference/usenixsecurity21/presentation/shen-kaiwen

这篇论文包含在第 30 届 USENIX 安全研讨会论文集中。

2021 年 8 月 11–13 日

978-1-939133-24-3

开放获取第 30 届 USENIX 安全研讨会论文集

由 USENIX 赞助。

身份验证链中的薄弱环节：电子邮件发件人欺骗攻击的大规模分析

沈凯文[1,*]， 王楚涵[1,*]， 郭明磊[1]， 郑晓峰[1,2,†]， 卢超一[1]， 刘宝军[1,†]赵宇轩[4]、豪爽[3]、段海欣[1,2]、潘庆峰[5]、杨敏[6]

[1]清华大学[2]齐安鑫技术研究院[3]德克萨斯大学达拉斯分校
[4]华北计算技术研究所[5]科威科技股份有限公司[6]复旦大学

摘要

电子邮件作为一种基本的通信服务，在个人和企业通信中发挥着重要作用，这也使其成为最常见的攻击媒介之一。电子邮件的真实性基于涉及多个协议、角色和服务的身份验证链，其中的不一致会造成安全威胁。因此，它取决于链条中最薄弱的环节，因为任何失败的部分都可能破坏整个基于链条的防御。

本文系统地分析了电子邮件的传输，并确定了一系列能够绕过 SPF、DKIM、DMARC 和用户界面保护的新型攻击。特别是，通过进行“鸡尾酒”联合攻击，可以伪造更真实的电子邮件来渗透著名的电子邮件服务，例如 Gmail 和 Outlook。我们对 30 个流行的电子邮件服务和 23 个电子邮件客户端进行了大规模实验，发现它们都容易受到某些类型的新攻击。我们已及时向相关电子邮件服务提供商报告发现的漏洞，并得到了其中 11 家的积极响应，包括 Gmail、雅虎、iCloud 和阿里巴巴。此外，我们还提出了抵御新攻击的关键缓解措施。因此，这项工作对于识别电子邮件欺骗攻击和提高电子邮件生态系统的整体安全性具有重要价值。

1 介绍

电子邮件服务一直是一种流行且必不可少的通信服务，具有丰富的个人和企业信息，这使其成为网络攻击的重点目标[22].然而，电子邮件传输协议远不能抵御潜在的攻击。电子邮件系统的安全性依赖于由各种电子邮件服务维护的多方信任链，这增加了系统对网络攻击的脆弱性。

正如木桶理论所揭示的那样，桶的容量取决于其最短的桶板。的真实性电子邮件取决于身份验证链中最薄弱的环节。当它集成到更广泛的系统中时，即使是无害的问题也可能造成前所未有的损害。通常，邮件认证链涉及多个协议、角色和服务，其中任何一个故障都可能破坏整个链式防御。

首先，尽管存在各种安全扩展协议（例如，SPF [24], DKIM [2] 和 DMARC [31]）识别欺骗邮件，由于受不同协议保护的实体不一致，欺骗攻击仍有可能成功。

其次，电子邮件的身份验证涉及四种不同的角色：发件人、收件人、转发者和 UI 呈现者。每个角色应承担不同的安全责任。如果任何角色未能提供适当的安全防御方案，则无法保证电子邮件的真实性。

最后，安全机制由处理策略不一致的不同电子邮件服务实现。此外，这些安全机制是由不同的开发人员实现的，其中一些在处理带有歧义标头的电子邮件时会偏离 RFC 规范。因此，不同服务之间存在许多不一致。攻击者可以利用这些不一致来绕过安全机制，并向网络邮件和电子邮件客户端呈现具有欺骗性的结果。

本文系统分析了邮件投递过程中认证的四个关键阶段：发送认证、接收认证、转发认证和UI渲染。我们发现了 14 种能够绕过 SPF、DKIM、DMARC 和用户界面保护的电子邮件欺骗攻击。通过组合不同的攻击，欺骗邮件可以完全通过所有流行的邮件安全协议，并且不会在收件人的 MUA 上显示任何安全警告。我们表明，即使对于具有高级技术背景的人来说，识别此类电子邮件是否是欺骗仍然具有挑战性。为了解欺骗性电子邮件攻击对电子邮件生态系统的真正影响，我们对 30 种流行的电子邮件服务进行了大规模实验，共有数十亿用户。此外，我们还在不同平台上测试了 23 款流行的电子邮件客户端

*两位作者对这项工作的贡献相同。
† 通讯作者：{zxf19, lbj15}@mails.tsinghua.edu.cn。

操作系统来衡量攻击对 UI 级别的影响。它们都容易受到某些类型的攻击，包括信誉良好的电子邮件服务，例如 Gmail 和 Outlook。我们已经及时向相关电子邮件服务提供商报告了所有发现的问题，并收到了其中 11 家（例如 Gmail、雅虎、iCloud、阿里云）的积极回应。

我们的工作显示了电子邮件生态系统中基于链的身份验证结构的脆弱性。这些攻击表明，更多的安全问题是由多方对安全机制的理解和实施不一致导致的。为了对抗电子邮件欺骗攻击，我们提出了一种 UI 通知方案。国内知名邮件服务商Coremail采用了我们的方案，并在用户的webmail和邮件客户端上实现。此外，我们还在 Github 上发布了我们的测试工具，供电子邮件管理员评估和提高他们的安全性。贡献。综上所述，我们做出以下贡献：

- 通过系统地分析电子邮件认证链，我们共识别出14种电子邮件欺骗攻击，其中9种（即A_3、A_6、A_7、A_8、A_9、据我们所知，A_{10}、A_{11}、A_{13}、A_{14}）是新的攻击。通过结合不同的攻击，我们可以伪造更真实的欺骗电子邮件来渗透著名的电子邮件服务，如 Gmail 和 Outlook。
- 我们对30 种流行的电子邮件服务和23 种电子邮件客户端进行了大规模测量。我们发现它们都容易受到某些攻击。我们负责任地披露了漏洞，并收到了 11 家电子邮件供应商（例如 Gmail、雅虎、iCloud 和阿里云）的积极回应。
- 为增强邮件系统对欺骗攻击的防护，我们提出了UI通知方案，并提供了邮件安全评估工具，供邮件管理员评估和提高其安全性。

2 背景

2.1 邮件投递流程

简单邮件传输协议（SMTP）[38] 是电子邮件服务的基本协议。数字1 显示了基本的电子邮件传递过程。发件人编写的电子邮件通过 SMTP 或 HTTP 协议从邮件用户代理（MUA）传输到邮件传输代理（MTA）。然后，发件人的 MTA 通过 SMTP 协议将电子邮件传输到收件人的 MTA，后者随后通过 HTTP、IMAP 或 POP3 将电子邮件内容传送到收件人的 MUA [27] 协议。

额外的传输需求可能会使实际交付过程复杂化。当原始电子邮件的目标收件人是邮件列表或配置了自动电子邮件转发时服务，电子邮件将通过电子邮件服务器进行中继，如图中的电子邮件转发服务器1.邮件转发服务器会修改收件人的地址并重新投递。

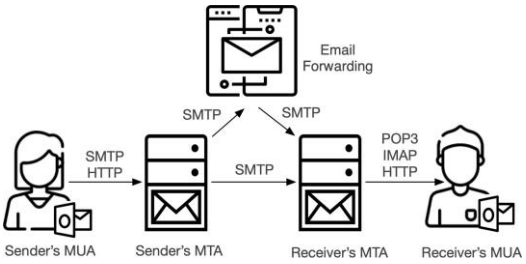


图 1：电子邮件传递过程。

在SMTP通信过程中，发件人的身份信息以复杂的方式包含在多个字段中。（1）Auth用户名，AUTH命令中使用的用户名，用于向服务器验证客户端。（2）MAIL From，信封上的发件人，主要用于邮件投递过程中的身份验证。（3）From，邮件正文中的发件人，是邮件客户端显示给用户的显示地址。（4)Sender，当From中有多个地址时，Sender字段用于识别真正的发件人。这些字段的不一致为电子邮件欺骗攻击提供了基础。

如图1，邮件传输过程中的认证涉及四个重要阶段。电子邮件发送验证。 MUA通过SMTP协议发送邮件时，发件人需要输入用户名和密码进行身份验证。这部分发件人的MTA不仅要验证用户身份，还要保证Mail From和Auth用户名一致。
电子邮件接收验证。当收件人的 MTA 收到邮件时，MTA 通过 SPF、DKIM 和 DMARC 协议验证发件人的真实性。见章节2.2.1 有关这些协议的详细信息。
电子邮件转发验证。邮件自动转发是另一种常用的邮件发送方式。当转发器自动转发电子邮件时，它应该验证发件人的地址。如果启用了 DKIM 签名，则最初的 DKIM 验证状态应为“通过”，然后添加新的 DKIM 签名。如果圆弧 [4]协议部署后，ARC验证链也将被验证。
电子邮件 UI 呈现。这个阶段是为用户提供一个友好的邮件渲染展示。不幸的是，大多数流行的电子邮件客户端的 UI 不会向用户显示真实性检查结果。一些编码格式或特殊字符可以用欺骗地址误导接收者。我们认为电子邮件 UI 呈现是身份验证过程中最后但也是关键的一步，这在以前的研究中经常被忽视。

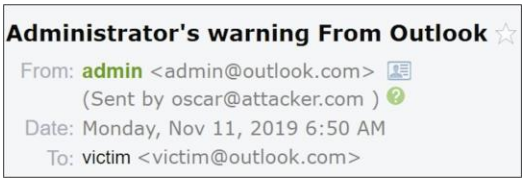


图 2：未通过发件人不一致检查的欺骗电子邮件。

2.2 电子邮件欺骗保护

2.2.1 电子邮件安全扩展协议

为了抵御电子邮件欺骗攻击，已经提出并标准化了各种安全扩展。目前应用最广泛的有SPF、DKIM和DMARC协议。防晒系数。发件人政策框架（SPF）[24]是一种基于IP的身份验证协议。它将发件人的域和IP地址一起标记和记录。收件人可以通过查询发件人域名对应的DNS服务器下的SPF记录来判断邮件是否来自申领域。
DKIM。域名密钥识别邮件（DKIM）[9]是一种基于数字签名的认证协议。它使用非对称密钥加密算法，允许发件人将数字签名添加到电子邮件的标头，以识别传输过程中的欺骗企图。收件人可以通过DNS查询获取发件人的公钥来验证签名，进而判断邮件是否被欺骗或篡改。
DMARC。基于域的消息认证、报告和一致性（DMARC）[31]是一个基于SPF和DKIM验证结果的认证系统。引入了多认证标识对齐机制，将From中的身份信息与SPF或DKIM认证标识相关联。同时，域所有者可以发布策略建议解决方案给收件人，以处理该域名发送的未经验证的电子邮件。域所有者可以定期从接收者那里得到反馈。具体来说，DMARC 对 SPF 和 DKIM 验证结果采用“或”状态检查。如果一封电子邮件通过了 SPF 或 DKIM 的检测，并且 From 可以与经过身份验证的标识符对齐，则它通过了 DMARC 的验证。

2.2.2 UI 级欺骗保护

UI 渲染是影响用户对电子邮件真实性感知的关键部分。然而，增加 UI 级别保护的必要性尚未培育出任何流行的安全协议。每个Email供应商采用不同的UI级别保护，目前还没有被广泛接受的全面保护机制。

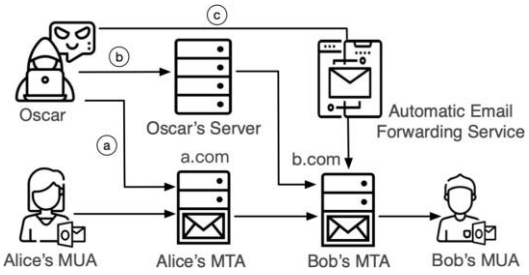


图 3：攻击模型：a、b 和 c 分别代表共享 MTA 攻击、直接 MTA 攻击和转发 MTA 攻击。

发件人不一致检查（SIC）。如图2，一些电子邮件服务添加了一个安全指示器来提醒接收者实际的发件人（MAIL From）可能不是显示的发件人（From）。值得注意的是，这种不一致性存在于整个电子邮件系统中，包括电子邮件转发、别名和电子邮件订阅。因此，收件人的 MTA 不能因为不一致而直接拒绝邮件，从而降低检测欺骗邮件的成功率。但是，针对该问题的保护措施在业界还没有得到明确的定义。我们将此保护措施定义为发件人不一致检查（SIC）。

3 攻击模型和实验

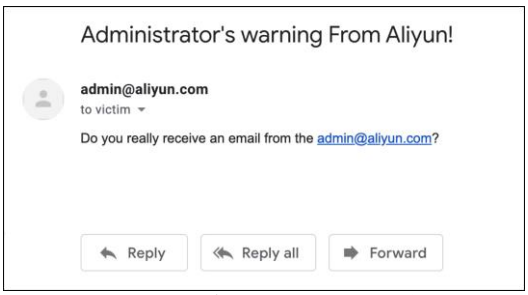
3.1 攻击模型

如图3，邮件欺骗攻击的攻击模型包括可信邮件发件人（Alice，拥有a.com下的邮件账号）、受害接收者（Bob，拥有b.com下的邮件账号）、敌手（Oscar）。具体来说，Oscar 的目标是向 Bob 发送一封电子邮件，进行欺骗爱丽丝@a.com并绕过所有安全验证。

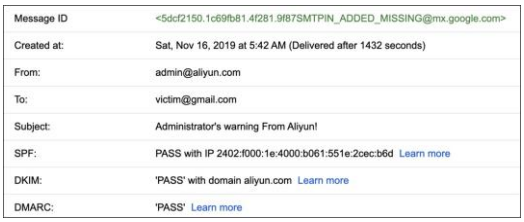
通常，存在三种常见的电子邮件欺骗攻击类型。

c 共享 MTA 攻击。我们假设 Oscar 有一个电子邮件帐户（Oscar@a.com），它不同于 Als 帐户（Alice@a.com）。Oscar 可以通过修改 Mail From/From/Auth 用户名标头，通过 a.com 的 MTA 发送欺骗性电子邮件。由于发件人 MTA IP 的可信度是影响垃圾邮件引擎决策算法的重要因素[5]，欺骗邮件很容易进入受害者的收件箱。发件人 MTA 的 IP 在 a.com 的 SPF 范围内。发件人的 MTA 也可能会自动将 DKIM 签名附加到欺骗电子邮件。因此，Oscar 绕过 SPF/DKIM/DMARC 验证和欺骗的难度不大爱丽丝@a.com。

b 直接 MTA 攻击。Oscar 还可以通过他自己的电子邮件服务器发送欺骗性电子邮件。注意发送方的MTA和接收方的MTA之间的通信过程



(a) Gmail 的网络用户界面不显示任何欺骗警报



(b) 欺骗邮件通过所有邮件安全协议验证

图 4：模拟的欺骗示例*admin@aliyun.com* 通过 Gmail。

没有身份验证机制。 Oscar 可以通过指定 Mail From 和 From 标头来欺骗任意发件人。这种攻击模型可以确保所有欺骗邮件都到达接收者的 MTA，而不受发件人 MTA 严格的发送检查的影响。

c 转发 MTA 攻击。 Oscar 可以滥用电子邮件转发服务来发送欺骗性电子邮件。首先，Oscar 可以向奥斯卡 @a.com,在转发电子邮件服务中属于 Oscar 的电子邮件帐户。接下来，他可以将转发服务配置为自动将此欺骗电子邮件转发给受害者 (Bob@b.com)。这种攻击模型具有三大优势。首先，这种攻击与共享 MTA 攻击模式具有相同的优势，因为接收方的 MTA (b.com) 认为邮件来自合法的 MTA (a.com)。此外，这种攻击还可以绕过发件人 MTA 的严格发送检查（例如，邮件发件人和发件人标头之间的不匹配）。最后，转发服务可能会为转发的电子邮件提供更高的安全背书（例如，添加不应添加的 DKIM 签名）。

因此，发件人认证问题可能发生在四个阶段，包括发送认证、接收验证、转发验证和UI渲染，这都可能构成潜在的安全威胁。

此外，我们将成功攻击的目标定义如下：（1）接收方的 MUA 错误地呈现发件人地址，因为它来自合法域名，而不是攻击者的真实域名；（2）收件人的 MTA 错误地验证了欺骗邮件的发件人；（3）收件人的 MUA 不显示任何欺骗电子邮件的安全警报。

数字4 显示成功的电子邮件发件人的示例

欺骗攻击使用直接 MTA 攻击和转发 MTA 攻击模型。攻击细节在章节中描述5. 三种电子邮件安全协议均对欺骗电子邮件给出“通过”验证结果。此外，接收者的 MUA 不会显示任何安全警报。受害者几乎无法从这种看似真实的欺骗电子邮件中识别出任何攻击痕迹。因此，即使对于具有高级技术背景的人来说，识别这样的电子邮件是否是欺骗也具有挑战性。

3.2 实验目标选择

我们系统地分析了 30 种电子邮件服务，包括最流行的免费公共电子邮件服务、企业级电子邮件服务和自托管电子邮件服务。我们的测试目标包括 Hu 等人测量的公共电子邮件服务。 [20】，除了不能在中国注册的（如 gmx.com和 sapo.pt），也没有有效的SMTP服务（如 tutanota.com和protonmail.com）。

我们总共选择了 22 种拥有超过 10 亿用户的流行电子邮件服务。我们相信他们的安全问题可能会使广泛的普通用户面临威胁。此外，我们还选取了Office 365、阿里云和Coremail等5家流行的企业邮箱来测试对机构用户的威胁效果。对于自托管电子邮件系统，我们构建、部署和维护了 3 个著名的电子邮件系统（即 Zimbra、EwoMail、Roundcube）。

此外，我们在不同的桌面和移动操作系统中测试了针对 23 个广泛使用的电子邮件客户端的攻击，以评估对 UI 渲染实现的影响。

3.3 实验方法

这项工作旨在涵盖整个电子邮件传递过程中所有可能的验证问题。因此，我们进行了五步实证安全分析：

首先，我们系统地分析电子邮件规范。在语法方面，我们提取 ABNF 规则 [10]，重点关注与身份验证相关的标头（例如，Mail From/From/Helo/Sender 标头）。我们还关注语义，特别是 RFC 中每个阶段的电子邮件身份验证。其次，我们收集合法的电子邮件样本，并根据 ABNF 语法生成带有身份验证相关标头的测试样本 [17]. 由于常见的电子邮件服务通常拒绝处理标题高度变形的电子邮件，因此我们为我们的经验实验目的指定了某些标题值。例如，我们将 domain 的值限制为几个著名的电子邮件域名（例如 gmail.com、icloud.com）。第三，我们介绍了协议模糊测试中常见的变异方法 [35]]，例如标头重复、插入空格、插入 Unicode 字符、标头编码和大小写变化。四、我们使用生成的样本来测试目标的安全验证逻辑

电子邮件系统分四个阶段。最后，我们分析和总结了使电子邮件发件人欺骗在实践中成功的对抗技术。

3.4 实验设置

在这项工作中，我们旨在总结针对已测试电子邮件服务的潜在电子邮件欺骗方法。因此，我们试图从第节提到的电子邮件传输过程的四个阶段找出所有验证问题2.下面，我们先分别介绍各个阶段的成功攻击。然后，我们讨论了我们为尽量减少测量偏差和避免伦理问题所做的努力。

成功的攻击。如果满足以下四个条件之一，我们认为电子邮件欺骗攻击成功。 (1) 在邮件发送认证阶段，攻击者可以任意修改标识符（如Auth username/MAIL From/From）。 (2) 在邮件接收验证阶段，即使欺骗域名已经部署了严格的SPF/DKIM/DMARC策略，但收件人的MTA给出了“none/pass”的验证结果。由于验证结果并不总是显示在电子邮件标题中，因此我们可以通过检查电子邮件是否已进入收件箱来推断结果。此外，如果我们的欺骗电子邮件被放入垃圾邮件箱，我们认为攻击失败，这意味着接收者的 MTA 已经检测到欺骗并采取了防御措施。为避免意外情况，我们将每次攻击重复 3 次，以确保欺骗电子邮件确实已穿透安全协议。 只有三次都有效的攻击才被认为是成功的攻击。 (3) 在邮件转发阶段，转发者对转发的邮件给予较高的安全背书。此外，如果攻击者可以在没有任何身份验证验证的情况下自由配置转发电子邮件到任何帐户，也可以认为攻击成功。 (4) 在邮件UI渲染阶段，显示的邮件地址与真实地址不一致。在这个阶段，我们使用 IMAP 的 APPEND 函数 [11] 协议将欺骗邮件发送到收件箱，因为我们只需要检查 UI 渲染结果而不是绕过垃圾邮件引擎。最后，我们收集信息并分析结果取决于 UI 级别的网络邮件和电子邮件客户端。

最小化测量偏差。首先，为了排除垃圾邮件检测的影响，我们选择了我们的行业合作伙伴，著名的电子邮件提供商提供的合法、良性和脱敏邮件样本作为我们的欺骗邮件的内容。这些邮件内容合法无害，不能判定为垃圾邮件。其次，所有的欺骗邮件都是从位于不同地区的15个IP地址以10分钟的间隔发送的。此外，我们为攻击者的域名和 IP 地址部署了 MX/TXT/PTR 记录。第三，为了测试接收者的 MTA 如何处理 SPF/DMARC 验证结果为“失败”的电子邮件，我们重现了 Hu 论文中的欺骗实验 [20] 在我们的目标上 30 个电子邮件服务。我们发现其中 23 家拒绝了 SPF/DMARC 验证结果为“失败”的电子邮件。其余的将它们标记为垃圾邮件。此外，结果表明，Hu 的论文中指出的大多数漏洞 [20】 这两年修好了。

伦理。我们已采取积极措施确保研究伦理。我们的测量工作仅使用我们自己拥有的专用电子邮件帐户。没有真正的用户受到我们实验的影响。我们还仔细控制了消息发送速率，间隔超过 10 分钟，以尽量减少对目标电子邮件服务的影响。

3.5 实验结果

这项工作将所有测试结果组织在表中1 和表2 提供发件人欺骗攻击的实验结果的一般情况。每次攻击和欺骗结果的详细信息在第4.我们将我们的实验结果总结如下。

首先，我们测量了这些电子邮件服务对电子邮件安全协议的部署和验证。所有电子邮件服务都在发件人端部署了 SPF 协议，而只有 23 种服务部署了所有这三种协议。令人惊讶的是，所有电子邮件服务都在接收方运行 SPF、DKIM 和 DMARC 检测。但是，只有 12 个服务执行发送方不一致检查。其次，所有目标电子邮件服务和电子邮件客户端都容易受到某些类型的攻击。最后，组合攻击允许攻击者伪造看起来更真实的欺骗电子邮件。

4 电子邮件发件人欺骗攻击

本节介绍电子邮件欺骗攻击中采用的各种技术。我们将攻击分为四类，对应于电子邮件传递过程中的四个身份验证阶段。

4.1 邮件发送认证攻击邮件发送验证是确保邮件真实性的必要步骤。对电子邮件发送身份验证的攻击可能会滥用知名电子邮件服务的 IP 信誉。他们甚至可以绕过 SPF/DKIM/DMARC 协议的所有验证，这对电子邮件安全生态系统构成了重大威胁。这些攻击主要用于共享攻击模型（模型a）。(

如节所述2.1，邮件发送过程中有3个发件人标识符：(1) Auth用户名； (2) 邮件发件人； (3) 从。在邮件发送验证过程中可以任意控制这些标识符的攻击被认为是成功的。

Auth 用户名和 Mail From 标头之间的不一致 (A_1)。如图5(a)，攻击者可以冒充当前域名下的任意用户发送

表 1：针对 30 个目标电子邮件服务的发件人欺骗实验结果。

电邮服务	协议部署			用户界面保护	电子邮件流四个阶段的弱点			
	防晒	DKIM	DMARC	标	发送中	接收	转发	界面渲染
Gmail.com		✓	✓	✓		A_6		A_{12}
众合网		✓	✓	✓	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}
邮箱.ru		✓	✓			A_4		A_{12}
雅虎网		✓	✓		A_2	A_3, A_7	A_{10}	A_{14}
腾讯网		✓	✓	✓	A_2	A_5		A_{13}, A_{14}
139.com		✓	✓	✓		A_4		A_{13}
搜狐网	✓				A_2	A_4, A_5	A_9	A_{13}
新浪网	✓				A_2	A_3, A_4, A_5, A_8		A_{13}, A_{14}
汤姆网		✓	✓	✓	A_2		A_9	
耶网		✓	✓	✓	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}
美国在线		✓	✓		A_2	A_5, A_7		A_{14}
Yandex.com		✓	✓			A_3, A_4,A_6, A_7, A_8	A_9	A_{14}
漫步者.ru		✓	✓		A_2	A_3		
Naver.com		✓	✓		A_2	A_4, A_5, A_8		
21世纪网	✓				A_2	A_4, A_5	A_9	
个人网	✓				A_2	A_4, A_5		
公鸡李		✓	✓		A_2	A_3, A_4		A_{13}, A_{12}
道姆网		✓	✓			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	
办公室 365		✓	✓	✓	A_2	A_4	A_9, A_{10},A_{11}	A_{14}
阿里云		✓	✓	✓	A_2	A_3, A_4, A_5, A_8	A_{10}	A_{13}
津布拉		✓	✓	✓	A_1, A_2	A_3, A_5, A_8	A_9	A_{12}, A_{13}
电子邮箱		✓	✓		A_2	A_3, A_4, A_8		A_{13}
圆立方体		✓	✓		A_1, A_2	A_3, A_4, A_8		A_{12}

[1] 下标标识特定的攻击（例如，A_8标识在中讨论的基于编码的攻击4.2).
[2] 缩写SIC代表receiver's sender inconsistency checks，providers自定义部署的邮件通知，在后台有介绍2.2.2.
[3] 带✓的情况表示该域名部署了相关的邮件安全协议或进行了发件人不一致检查。

邮件发送验证时Auth用户名（Oscar@a.com）和Mail From（Alice@a.com）不一致的欺骗邮件。 SMTP 协议不提供任何内置的安全功能来保证 auth 用户名和 Mail From 标头的一致性。因此，这种类型的保护仅取决于电子邮件开发人员的软件实现。

在我们的欺骗实验中，大多数电子邮件服务都注意到了此类问题，并禁止用户发送与其原始身份不一致的电子邮件。然而，此类问题仍然出现在一些知名的企业电子邮件软件（即 Zimbra、EwoMail）中。这两个电子邮件服务在默认安全配置下容易受到攻击。电子邮件管理员需要升级他们的安全配置以手动防止此类问题。

邮件发件人和发件人标头之间的不一致（A_2）。攻击者可以发送带有不同 Mail From 和 From 标头的欺骗性电子邮件。数字5(b) 显示了这种类型的攻击。尽管允许某些用户使用电子邮件别名发送具有不同 From 标头的电子邮件，但不应允许任何用户随意将 From 标头修改为任何值（例如，admin@a.com）以防止攻击。 From 标头只允许在有限的合法值内设置。许多流行的电子邮件服务（如 Outlook、新浪、QQ 邮件）和大多数第三方电子邮件客户端（如 Foxmail、Apple Mail）仅显示 From 标题，而不显示 Mail From 标题。对于这些具有不同 Mail From 和 From 标头的电子邮件，受害者甚至无法在 MUA 上看到任何安全警报。

RCPT To 和
到标题。在现实世界中，有一些场景

表 2：23 个目标电子邮件客户端的发件人欺骗实验结果。

操作系统	客户	标准集成电路	弱点
视窗	邮箱	✓	A_6, A_7, A_{13}, A_{14}
	外表	✓	A_6, A_{13}
	电子商务客户端	✓	A_6, A_{12}
	Windows 邮件		A_6, A_{13}, A_{14}
苹果系统	邮箱		A_6, A_{13}
	外表	✓	A_6, A_{13}
	电子商务客户端	✓	$A_6, A_7, A_{12}, A_{13}, A_{14}$
	苹果邮件		A_6, A_{13}, A_{14}
Linux目	雷鸟		A_6, A_{13}
	邮寄弹簧		A_6, A_{13}, A_{14}
	爪甲		A_6, A_{14}
	进化		A_6, A_{13}, A_{14}
	仙女座		A_6, A_{13}, A_{14}
安卓	电子邮件		A_6, A_{13} A_6,
	QQ邮箱 网易邮箱	✓	A_{13}, A_{14} A_6, A_{12}, A_{13}
	外表	✓	A_6, A_{13}
苹果	邮件.app		A_6, A_7, A_{13}, A_{14}
	QQ邮箱 网易邮箱	✓	A_6, A_{13} A_6, A_{12}, A_{13}
	外表	✓	A_6, A_{13}

[1] 下标标识特定的攻击。
[2] SIC 代表发送方不一致检查。
[3] 带有 ✓ 的情况表示电子邮件客户端执行发件人不一致检查。
[4] 由于电子邮件客户端不涉及邮件协议的验证，我们只测试了与电子邮件 UI 渲染相关的攻击（即 A6、A7、A12、A13、A14）。

导致不一致，例如电子邮件转发和密件抄送。然而，这种灵活性增加了攻击面并引入了新的安全风险。例如，攻击者可以向受害者发送电子邮件，即使电子邮件的收件人标头不是受害者的地址。在这种情况下，攻击者可以进一步利用该方法获取正常情况下无法获取的带有DKIM签名的欺骗邮件，这有助于进一步的攻击。该技术单独使用时可能效果不佳，但与其他攻击技术结合使用时，往往可以取得出色的欺骗效果。

在我们的实验中，有 14 种电子邮件服务容易受到此类攻击。此外，我们还发现一些电子邮件服务（如 Outlook、Zoho、AOL、Yahoo）已经意识到这些风险并实施了相应的安全限制。在 SMTP 发送过程中，他们拒绝发送 Mail From 和 From 标头不一致的电子邮件。然而，这些防御仍然可以被两种类型的攻击（即 A_4、A_5）绕过。例如，我们可以发送一个欺骗

(a) 使用不同的身份验证用户名和邮件发件人标头进行攻击

(b) 使用不同的 Mail From 和 From 标头进行攻击

图 5：两次绕过发送服务验证的攻击。

带有 Mail From 标头的电子邮件为<奥斯卡@a.com>和 From 标头为<爱丽丝@a.com,奥斯卡@a.com>在 Yahoo 中引入了另一个歧义源并最终绕过了电子邮件协议验证。因此，即使发件人已采取相关安全措施，仍有可能发送此类欺骗性电子邮件。

4.2 邮件接收验证攻击

SPF、DKIM 和 DMARC 是用于对抗电子邮件欺骗攻击的普遍机制。如果攻击者可以绕过这些协议，也可能对电子邮件安全生态系统造成严重的安全威胁。发起此类攻击的攻击模型有三种：共享MTA攻击、直接MTA攻击和转发MTA攻击。当接收方的 MTA 错误地获得“无/通过”验证结果时，攻击就成功了。

来自攻击的空邮件（A_3）。 RFC 5321 [25] 明确说明允许一个空的Mail From，主要用于防止退回环回和允许一些特殊的消息。但是，此功能也可能被滥用以发起电子邮件欺骗攻击。如图6，攻击者可以发送一封带有空 Mail From 标头的电子邮件，而 From 标头会伪造 Alice 的身份（Alice@a.com）。

SPF协议[23]规定如果Mail From头为空，接收方的MTA必须根据Helo字段完成SPF验证。然而，现实生活中Helo字段的滥用使得一些邮件服务违背了标准，采用了更加宽松的验证方式。这样，收件人在处理这些邮件时，无法根据Helo字段完成SPF验证，而是直接返回“none”。这种类型的错误允许攻击者绕过 SPF 保护。因此，攻击者可以将此攻击的 SPF 结果从“失败”更改为“无”。

13 种电子邮件服务（例如 Yahoo、Yeah、126、Aol）容易受到此类攻击。幸运的是，已经有 17 家电子邮件服务解决了此类安全问题，其中 5 家

图 6：来自绕过 SPF 验证的攻击的空邮件。

(a) 普通多重From攻击。 (b) 多个来自空格的攻击。

(c) 多重来自攻击与案例变化。 (d) 多个来自攻击与不可见人物。

图 7：使 DMARC 验证的多重 From 攻击奥斯卡@attack.com而 MUA 显示爱丽丝@a.com。

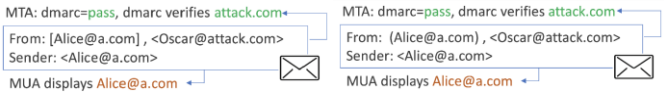
其中（例如 Zoho.com、iCloud.com、exmail.qq.com）将此类电子邮件放入垃圾邮件。

多个来自标头（A_4）。受 Chen 等人的工作启发。 [6]，我们还在电子邮件欺骗攻击中使用了多个标头技术。与 Chen 的工作相比，我们有更多来自 From 标题的扭曲，例如在 From 前后添加空格、大小写转换和插入不可打印的字符。如图7，攻击者可以构造多个 From 标头来绕过安全策略。 RFC 5322 [40] 表示具有多个发件人字段的电子邮件通常会被拒绝。但是，仍然有一些电子邮件服务未能遵循该协议并接受具有多个发件人标头的电子邮件。它可能会在电子邮件接收验证阶段引入不一致，这可能会导致额外的安全风险。数字7(c) 显示了一个示例，显示的发件人地址是爱丽丝@a.com,而接收方的 MTA 可能会使用奥斯卡@attack.com用于 DMARC 验证。

只有 4 种邮件服务（即 Gmail、Yahoo、Tom、Aol）拒绝具有多个 From 标头的电子邮件，并且有 19 种邮件服务受到此类攻击的影响。大多数测试的电子邮件服务倾向于在网络邮件上显示第一个发件人标头，而 6 种服务（例如 iCloud、Yandex、阿里云）选择显示最后一个发件人标头。此外，已有7家厂商针对此类攻击制定了具体的安全规定，例如在webmail上同时显示两个发件人地址（如QQ邮箱、Coremail）或将此类邮件放入垃圾邮件文件夹（如Outlook、rambler.ru）。

多个电子邮件地址（A_5）。使用多个电子邮件广告-

(a) 普通的多地址攻击。 (b) 多地址攻击 null 地址。



(c) Multiple address attack with seman-(d) 多地址攻击与 com-抽动字符。 评论。

图 8：多个电子邮件地址攻击使 DMARC 验证奥斯卡@attack.com而 MUA 显示爱丽丝@a.com。

连衣裙也是绕过协议验证的有效技术。多地址的使用首先在 RFC2822 [39] 并且在 RFC 5322 [40].它适用于这样的场景：一封电子邮件

多个作者应该在 From 标题中列出所有作者。然后，添加发件人字段以标记收件人
真正的发件人。如图8(a)，攻击者可以绕过具有多个电子邮件地址的 DMARC 验证（<Alice@a.com>, <Oscar@attack.com>).此外，我们还可以对这些地址进行一些基于规则的突变，比如[Alice@a.com], <Oscar@attack.com>.

15邮箱服务（如QQ邮箱、21cn.com和onet.pl）仍将接受此类邮件。只有 4 个服务（例如 Gmail 和 Mail.ru）直接拒绝这些电子邮件，而其他 5 个服务（例如 zoho.com、tom.com、outlook.com）将它们放入垃圾邮件。其余 6 项服务（例如 139.com、cock.li 和 Roundcube）显示所有这些地址，使欺骗电子邮件更难欺骗受害者。

解析不一致攻击（A_6）。邮件发件人和发件人标头采用富文本格式，语法格式非常复杂。因此，正确解析显示名称和真实地址具有挑战性。这些不一致可以让攻击者绕过身份验证并欺骗他们的目标电子邮件客户端。

邮箱地址是这两个标头的基本组成部分之一。首先，允许邮箱地址有路由部分[39] 当用“<”和“>”括起来时，在真实发件人地址前面。因此，邮箱（<@a.com,@b.com:admin@c.com>）仍然是一个合法的地址。其中，@a.com、@b.com为路由部分，“admin@c.com" 是真正的发件人地址。其次，允许使用邮箱列表和地址列表[39]，它们可以有“空”成员，例如 <a@a.com>, ,<b@b.com>.三、评论[40] 是用括号括起来的字符串。它们允许位于本地部分和域的以句点分隔的元素之间，例如 <admin(username)@a.com(domain name)>。最后，还有一个可选的显示名称 [40] 在 From 标头中。它表示发件人的姓名，显示给收件人。数字9 显示三种类型的攻击

(a) 解析与路由部分不一致。

（b）解析与“空”邮箱列表不一致。

（c）解析与评论不一致。

（d）NUL 字符截断字符串解析。

（e）不可见的 unicode 字符截断字符串解析。

(f) 语义字符截断字符串解析。

图 9：六个绕过接收服务验证的欺骗示例。

(a) 基于编码的攻击绕过 DMARC 验证。

(b) 组合编码和截断攻击。

图 10：两个基于编码的攻击的欺骗示例。

基于解析不一致。

截断字符是终止字符串解析的一系列字符。在从邮件标题中解析和提取目标域名时，截断字符将结束解析过程。数字9(d) 显示程序在从字符串解析目标域名时得到了一个不完整的域名（a.com）"admin@a.com x00@attack.com”。攻击者可以使用这些技术来绕过电子邮件安全协议的验证。总的来说，这项工作在电子邮件字符串解析过程中发现了三种类型的截断字符。首先，NUL（x00）字符可以终止 C 编程语言中的字符串。它在电子邮件领域具有相同的效果。其次，一些不可见的 Unicode 字符（例如 uff00-uffff、x81-xff）也可以终止字符串解析过程。第三，某些语义字符，如“[],{,}, t, r, n,;”，可以用来表示语法分析中的分词点。同时，这些字符也影响了字符串的解析过程。

我们发现有 13 个电子邮件服务在此类攻击下的 UI 渲染阶段存在问题。对于Gmail和Yandex，我们可以利用这些攻击技术来绕过DMARC。基于编码的攻击（A_7）。RFC 2045(MIME)［15］描述了一种表示文本正文部分的机制，这些部分以各种字符集编码。这些的ABNF文法部分如下：=?charset?encoding?encoded-text?=。“charset”字段指定与未编码文本关联的字符集；“encoding”字段指定编码算法，其中“b”表示base64编码，“q”表示quoted-printable编码；“编码文本”字段指定编码文本。攻击者可以使用这些编码地址来逃避电子邮件安全协议验证。数字10(a) 显示了此类攻击的详细信息。对于编码地址，例如 From: =?utf-8?b?QWxpY2VAYS5jb20=?=，大多数电子邮件服务在验证 DMARC 协议之前不会对地址进行解码，因此无法提取准确的域并在中得到“无”以下 DMARC 验证。但是，某些电子邮件服务会在 MUA 上显示解码后的发件人地址（Alice@a.com）。此外，这种技术可以与截断的字符串结合使用。如图所示10(b)，攻击者可以将 From 标头构造为"b64(Alice@a.com>b64(uffff)@attack.com”。电子邮件客户端程序可能会获得不完整的用户名（即 Alice@a.com），但它仍会使用攻击者的域（attack.com）进行 DMARC 验证。

7 个电子邮件服务受到该漏洞的影响，包括一些拥有超过 10 亿用户的流行服务（例如 Outlook、Office 365、雅虎）。

子域攻击（A_8）。攻击者可以从知名电子邮件服务（例如 admin@mail.google.com）的不存在的子域（无 MX 记录）发送欺骗性电子邮件。因此，没有相应的 SPF 记录。欺骗邮件只会得到“None”的验证结果，收件人的MTA不会直接拒绝。尽管父域（例如 google.com）部署了严格的电子邮件策略，但攻击者仍然可以通过这种方式进行攻击。不幸的是，许多公司使用子域来发送业务订阅电子邮件，例如 Paypal、Gmail 和 Apple。因此，普通用户倾向于信任此类电子邮件。

不幸的是，RFC 7208［24］声明不鼓励使用通配符记录发布 SPF 记录。很少有电子邮件管理员在现实世界中配置通配符 SPF 记录。此外，收件人的 MTA 通常可以拒绝来自没有 MX 记录的域的电子邮件。但是RFC

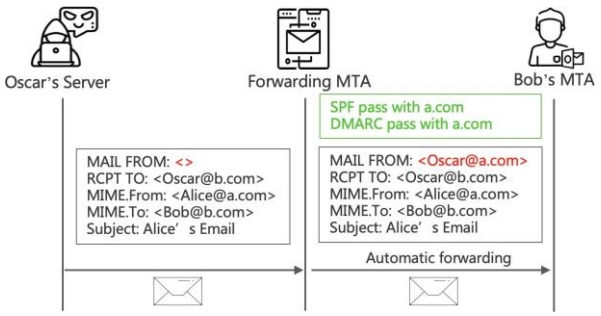


图 11：利用转发服务绕过 SPF 和 DMARC。

2821 [26] 提到，当域没有 MX 记录时，SMTP 假定 A 记录就足够了，这意味着任何具有 A 记录的域名都可以被视为有效的电子邮件域。此外，很多知名网站都部署了通配符DNS A记录，使得此类攻击的适用性更高。因此，收件人的 MTA 很难确定是否拒绝此类邮件。

实验结果表明，有 13 种电子邮件服务容易受到此类攻击。在我们的实验中，只有一个电子邮件服务 (Mail.ru) 为 SPF 记录部署了通配符 DNS 条目。默认情况下，为组织域设置的 DMARC 策略应适用于任何子域，除非已为特定子域发布 DMARC 记录。然而，实验结果表明，即使接收方的 MTA 进行了 DMARC 检查，我们的攻击仍然有效。

4.3 电子邮件转发验证中的攻击这项工作表明，攻击者可以滥用电子邮件转发服务来发送在共享 MTA 攻击模型中会失败的欺骗电子邮件。此外，转发服务可以为转发的邮件提供更高的安全背书。攻击者可以利用这两种情况发送欺骗性电子邮件。未经授权的转发攻击 (A_9)。如果攻击者可以随意配置转发邮件到任何账户而无需任何身份验证，则电子邮件服务存在未授权转发问题。首先，攻击者应该在电子邮件转发服务上拥有合法的电子邮件帐户。因为这些邮件是从知名的邮件转发MTA发出的，所以收件人的MTA一般都会接受此类邮件。当目标域名与转发域名相同时，我们还可以利用转发服务绕过 SPF 和 DMARC 协议。这种攻击如图所示11.基于这种攻击，攻击者可以滥用知名 MTA 的可信度来制作逼真的欺骗电子邮件。

在我们的实验目标中，有 12 个电子邮件服务存在此类漏洞。 7 电子邮件服务不提供电子邮件转发功能。其他邮件服务已经意识到风险并进行了相应的转发验证修理它。

DKIM 签名欺诈攻击 (A_{10})。转发服务可以为转发的电子邮件提供更高的安全背书。但是攻击者可以滥用此功能来发送欺骗性电子邮件。如果转发的邮件没有 DKIM 签名或之前未通过 DKIM 验证，则转发者不应添加其域名的 DKIM 签名。否则，攻击者可以骗取合法 DKIM 签名的转发服务。然而，RFC 6376 [34] 和 RFC 6377 [30] 建议转发者在转发的邮件中加上自己的签名。这进一步导致更多的电子邮件服务出现此类问题。

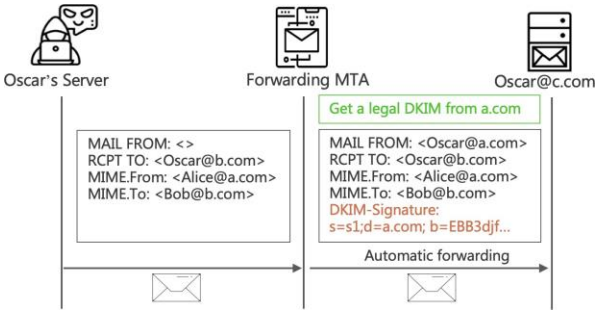
数字12 说明了攻击的完整过程。电子邮件转发服务 (a.com) 在没有严格验证的情况下对所有转发的电子邮件进行签名并添加 DKIM 签名。首先，攻击者可以在电子邮件转发服务下注册一个帐户 (Oscar@a.com)。其次，他可以配置所有接收电子邮件转发到另一个攻击者的电子邮件地址 (Oscar@c.com)。然后，攻击者可以发送一封带有发件人的欺骗性电子邮件：爱丽丝@a.com，到：鲍勃@b.com到奥斯卡@a.com 通过直接 MTA 攻击模型。转发服务 (a.com) 向此欺骗电子邮件添加合法的 DKIM 签名。因此，攻击者会收到一封带有由 a.com 签名的合法 DKIM 签名的欺骗性电子邮件。在我们的实验中，阿里云、Office 365 和雅虎邮箱都容易受到此类攻击。

ARC 问题 (A_{11})。圆弧 [4] 是一个新提出的协议，它提供了一个信任链来链接电子邮件转发过程中SPF、DKIM和DMARC的验证结果。在我们的实验中，只有三种电子邮件服务 (即 Gmail、Office 365 和 Zoho) 部署了 ARC 协议。然而，我们的研究发现 Office 365 和 Zoho 都存在 ARC 协议实施的安全问题。此外，除了A_{10}攻击外，ARC 无法防御上述大多数攻击。

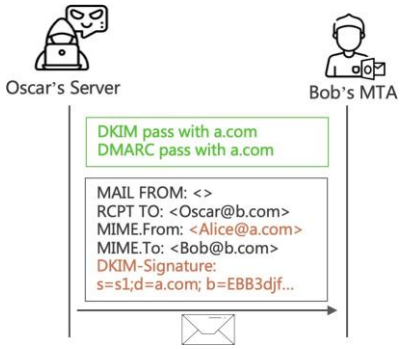
对于 Zoho 电子邮件服务，如果电子邮件未通过发件人不一致检查，它会向用户显示警报。但是，Zoho 的 ARC 实现有一个错误。当欺骗性电子邮件通过 Gmail 自动转发到 Zoho 邮箱时，Zoho 添加的 ARC-Authentication-Results (AAR) 标头显示错误的“通过”DMARC 验证结果。更糟糕的是，这种不正确的 ARC 实现还可以绕过发送方不一致检查。 Zoho 不会针对此欺骗性电子邮件向用户显示警报。 Office 365 在 ARC 的实现上也存在错误。它通过了 AAR 头中 SPF、DKIM 和 DMARC 的错误验证结果。这会破坏 ARC 信任链，从而带来更多安全风险。

4.4 电子邮件 UI 渲染中的攻击

电子邮件系统的最后也是最关键的部分是确保正确呈现电子邮件。一旦攻击者能够攻破这个阶段的防御措施，普通用户就很容易



(a) 欺骗邮件骗取a.com签名的DKIM签名。



(b) 使用合法的 DKIM 签名进行欺骗。

图 12：利用转发服务绕过 DKIM 和 DMARC。

在不知不觉中被这种欺骗性的电子邮件所欺骗。

显示的地址是 MUA 上显示的发件人地址，但真实地址是 SMTP 通信中使用的发件人身份（发件人）。如果攻击者能够使显示的地址与真实地址不一致，则认为攻击成功。此外，如图所示2，一些 MUA 为那些未通过发件人不一致检查的电子邮件添加安全指示器。如果攻击者能够绕过发送方不一致性检查，也被认为是一种有效的攻击技术。

电子邮件 UI 渲染阶段存在各种攻击。有些类似于前面讨论的 A_6、A_7攻击。不同的是，UI 级攻击的目标是绕过发件人不一致检查和欺骗显示给用户的电子邮件地址，而不是绕过三种电子邮件安全协议的验证。因此，我们通常构造模棱两可的 From 标头而不是 Mail From 标头。在本节中，我们只讨论前面没有提到的攻击技术。

IDN 同形异义词攻击（A_{12}）。同形异义词攻击［16］是一个已知的网络安全问题，但尚未系统地讨论其对电子邮件系统的安全风险。随着流行的电子邮件提供商逐渐支持来自国际化域名（IDN）的电子邮件，这种攻击可能会产生更广泛的安全影响。

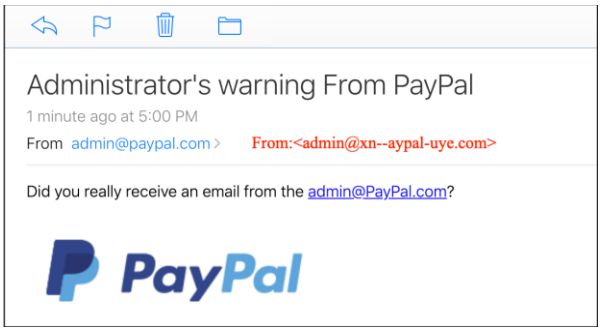


图 13：IDN 同形异义词攻击冒充示例 *admin@paypal.com* 在 iCloud.com 网页界面上。

Punycode 是一种将无法在 ASCII 中显示的单词转换为 Unicode 编码的方法。值得注意的是，Unicode 字符在屏幕上的外观可能相似，但原始地址不同。数字13显示一封看似来自地址（admin@paypal.com），但实际上来自地址（admin@xn--aypal-uye.com）的欺骗性电子邮件。

现代浏览器已经针对 IDN 同形异义词攻击实施了一些防御措施。例如，如果域标签包含来自多种语言的字符，则不应呈现 IDN。不幸的是，我们在电子邮件系统中几乎没有发现类似的防御措施。

实验结果显示，显示了 10 个支持 IDN 电子邮件的电子邮件服务（例如 Gmail、iCloud、Mail.ru）。目前只有Coremail修复了该漏洞。在我们的帮助下，Coremail 在地址栏中的 Unicode 字符前后添加了空格。通过这种方式，用户可以轻松区分 ASCII 字符和 Unicode 字符，从而防止此类攻击。

缺少 UI 渲染攻击（A_{13}）。我们还发现许多字符会影响 MUA 的渲染。在渲染过程中可能会丢弃一些字符。此外，某些字符也可能导致电子邮件地址被截断（类似于攻击 A_6）。这些字符包括不可见字符（U+0000-U+001F,U+FF00-U+FFFF）和语义字符（@,:,;,″）。例如 MUA 渲染地址 admin@gm@ail.com 作为admin@gmail.com。仍有 12 家电子邮件服务（例如 zoho.com、163.com、sohu.com）容易受到此类攻击。其他服务拒绝接收或只是将此类电子邮件扔进垃圾邮件箱。从右到左的覆盖攻击（A_{14}）。几个字符被设计用来控制字符串的显示顺序。其中之一是“从右到左覆盖”字符 U+202E，它告诉计算机以从右到左的顺序显示文本。它主要用于书写和阅读阿拉伯语或希伯来语文本。虽然这种攻击技术[1]已在其他地方讨论过，其对电子邮件欺骗的安全风险尚未得到充分探讨。攻击者可以构造一个字符串为 alice，@a.com 显示

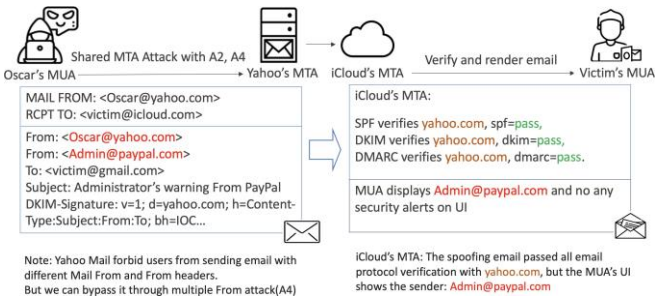


图 14：结合 A_2和 A_4攻击来冒充*admin@paypal.com* 在 iCloud 上。

作为爱丽丝@a.com。因为带有RTL字符的欺骗邮件可能会被直接扔进垃圾邮件箱，所以我们一般对payload进行编码（使用utf-8模式）进行攻击。

11 种电子邮件服务（例如 Outlook、Yahoo、Yandex）仍然容易受到这种攻击。 10 项服务（例如 cock.li、daum.net、onet.pl）无法正确呈现此类电子邮件地址。其他电子邮件服务直接拒绝此类邮件。

5 联合攻击

根据电子邮件传递过程中的四个身份验证阶段，我们将攻击分为四类。然而，这些攻击有一定的局限性。首先，某些攻击（例如 A_2、A_3）可能会对处方产生欺骗效果。但是，他们无法绕过所有电子邮件欺骗保护。例如，通过 Empty Mail From Attack (A_3) 发送的欺骗邮件绕过了 SPF 验证，但未能通过 DMARC 验证。此外，大多数电子邮件供应商已经修复了单独进行的攻击，这些攻击可以绕过我们实验中的所有三种电子邮件安全协议。因此，结合不同阶段的多次攻击在实践中更为可行。通过结合不同攻击技术的“鸡尾酒”联合攻击，我们可以轻松构造出完全通过三种电子邮件安全协议和用户界面保护验证的欺骗邮件。最后， 这封欺骗电子邮件与合法电子邮件之间的收件人 MUA 没有显示差异。

通过在4个认证阶段结合3种攻击模型和14种攻击技术，可以产生大量可行的组合攻击。这项工作选择了两个最具代表性的例子来说明联合欺骗攻击的效果。桌子3 列出了两个示例的关键信息。

同一攻击模型下的联合攻击。我们共识别出14种邮件欺骗攻击技术，其中14种攻击技术可以在同一种攻击模型下进行组合，以达到更好的攻击效果。此外，虽然一些供应商可能通过一次安全检查修复漏洞，但攻击者可以准确地结合其他绕过相应安全检查的攻击技术。

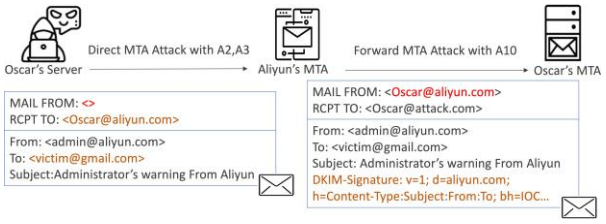
数字14 显示了共享 MTA 攻击模型下的代表性示例。Yahoo 电子邮件执行简单的发件人检查策略来防御 A_2攻击。它禁止用户发送具有不同 Mail From 和 From 标头的电子邮件。但是，攻击者仍然可以通过 A_4攻击绕过此发件人检查策略。具体来说，我们可以发送带有第一个 From 标头 (Oscar@yahoo.com) 的欺骗电子邮件，这与 Mail From 标头相同。然后，我们添加第二个发件人标头 (Admin@paypal.com)。有趣的是，iCloud 不会拒绝此类具有多个发件人标头的欺骗电子邮件。更糟糕的是，iCloud 使用第一个 From 标头执行 DMARC 验证并通过 yahoo.com 获得“通过”结果，而第二个 From (Admin@paypal.com) 标头显示在用户的网络邮件 UI 上。因此，这种组合攻击最终可以绕过所有三种电子邮件安全协议并欺骗 MUA。不同攻击模型下的联合攻击。 攻击者还可以通过组合不同的攻击模型来进行更有效的攻击。邮件系统是一个复杂的多方信任链生态系统，依赖于多方实施和部署的安全措施。在不同的攻击模型下，多方可能存在各种漏洞。例如，如果电子邮件服务的发送MTA在发送验证时进行严格检查，则很难通过共享MTA攻击模型进行攻击。但是，一旦在其他阶段未能提供正确完整的安全防御方案，攻击者仍然可以通过其他两种攻击模型绕过并发送欺骗邮件。因此，通过组合多种攻击模型，我们在现实世界中有更多的组合攻击。

数字4 通过结合直接和转发 MTA 攻击模型显示成功的欺骗攻击。例如，Oscar 使用攻击技术 (A_2,A_3) 发送带有空邮件发件人和精心制作的发件人标题的欺骗电子邮件。此外，Oscar 还有一个合法的账号 (Oscar@aliyun.com)，与受害者的账号不同。因此，Oscar 可以将此帐户配置为自动将收到的电子邮件转发到他的帐户之一 (Oscar@attack.com)。阿里云服务会为所有转发的邮件添加 DKIM 签名，而无需进行必要的验证检查 (A_{10})。它授予 Oscar 的欺骗电子邮件合法的 DKIM 签名。然后，Oscar 可以使用 Mail 发送此欺骗性电子邮件来自：<admin@attack.com>通过直接 MTA 攻击模型标头，如图所示15(b).

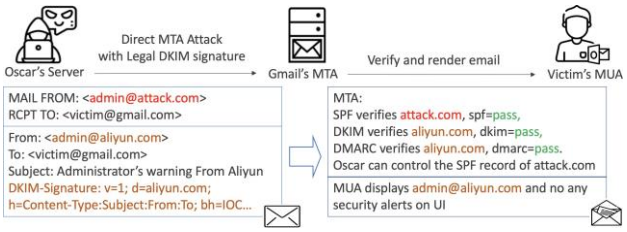
对于此欺骗邮件，SPF 协议验证 attack.com 域，而 DKIM 和 DMARC 协议验证 aliyun.com 域。因此，这封邮件可以通过所有的三个邮件安全协议，进入Gmail的收件箱。此外，没有电子邮件服务会向用户显示有关具有三种协议的不同验证域的电子邮件的警报。进一步使此类攻击对普通用户更具欺骗性。

表 3：两个组合攻击示例的详细信息。

攻击	从	到	攻击模型	组合攻击
情况1	admin@paypal.com	受害者@icloud.com	共享 MTA 攻击	$A_2 + A_4$
案例二	admin@aliyun.com	受害者@gmail.com	直接和转发 MTA 攻击	$A_2+A_3+A_{10}$



(a) 第一阶段攻击获得了阿里云合法的DKIM签名。



(b) 第二阶段的攻击通过了Gmail的三个邮件协议安全验证。

图 15：来自 A_2、A_3和 A_{10}的组合攻击admin@aliyun.com到受害者@gmail.com。

6 根本原因和缓解措施

6.1 根本原因

如前所述，电子邮件系统的安全性依赖于由多方分别执行的多项保护策略。因此，这些多方的不一致可能会产生更多漏洞并导致严重的欺骗攻击。我们确定攻击的根本原因如下。

多协议之间的薄弱环节。由于电子邮件规范的模糊性、最佳实践的缺乏以及 MIME 标准的复杂性，协议验证过程是身份验证链中的薄弱环节之一。在SMTP通信过程中，协议的多个字段包含了发送者的身份信息（即Auth用户名、MAIL From、From、Sender）。这些字段的不一致为电子邮件欺骗攻击提供了基础。

SPF、DKIM、DMARC被提出并标准化，从不同方面防止邮件欺骗攻击。但是，只有当所有协议都得到很好的执行时，电子邮件系统才能防止电子邮件欺骗攻击。在这种基于链的认证结构中，任何一个环节的故障都可能导致认证链失效。

多角色之间的薄弱环节。在电子邮件系统中，验证发件人的身份是一个复杂的过程。它涉及四个重要角色：发送者、接收者、转发者和UI渲染者。标准安全模型的工作假设是每个角色都适当地开发和实施相关的安全验证机制以提供整体安全性。但是，许多电子邮件服务并未在所有四个角色中实施正确的安全策略。

许多邮件服务（如iCloud、Outlook、Yeah.com）在邮件转发阶段并没有注意到未经授权的转发攻击（A_9）带来的安全风险。此外，规范并未明确说明电子邮件安全验证中四个角色（即发送者、接收者、转发者和UI渲染者）的职责。

多服务之间的薄弱环节。不同的电子邮件服务通常具有不同的配置和实现。某些服务（例如 Gmail、Yandex.com）禁止发送标题不明确的电子邮件，但可以容忍地接收它们。相反，一些（例如 Zoho、Yahoo）倾向于允许发送带有模糊标题的电子邮件，但在电子邮件接收验证阶段进行非常严格的检查。安全策略之间的差异允许攻击者从具有容忍发送策略的服务向具有松散接收策略的服务发送欺骗电子邮件。

此外，一些电子邮件提供商在处理标头不明确的电子邮件时会偏离 RFC 规范。当 MUA 处理多个 From 标头时，一些服务（例如 Outlook、Mail.ru）显示第一个标头，而其他服务（例如 iCloud、yandex.com）显示最后一个标头。

此外，不同的供应商对 Unicode 字符的支持程度不同。一些厂商（如21cn.com、Coremail）已经意识到Unicode字符带来的新的安全挑战，但一些厂商（如163.com、yeah.net）则一无所知。特别是一些（例如zoho.com、EwoMail）甚至还不支持Unicode字符的渲染。

最后，只有少数电子邮件提供商显示视觉 UI 通知以提醒用户欺骗电子邮件，并且只有 12 家供应商实施发件人不一致检查。特别是，由于缺乏统一的实施标准，实践中的发送方不一致检查存在很大差异。缺乏有效合理的邮件安全通知机制，也是邮件欺骗屡屡被禁止，却从未根除的原因之一。

6.2 减轻

本小节讨论关键的缓解措施。由于电子邮件欺骗是一个涉及多方的复杂问题，因此需要多方协作来应对相关问题。

更准确的标准。请注意，由于电子邮件协议中的定义不明确，电子邮件提供商可能无法提供安全可靠的电子邮件服务。因此，提供更准确的电子邮件协议描述对于消除多方协议实践中的不一致是必要的。例如，DKIM 标准应指定何时应将 DKIM 签名添加到转发的电子邮件中。转发者添加DKIM签名以提高邮件的可信度是合理的；但是，他们不应将 DKIM 签名添加到从未通过 DKIM 验证的电子邮件中。

用户界面通知。电子邮件 UI 呈现是影响用户对电子邮件真实性感知的重要部分。不幸的是，我们实验中的大多数网络邮件和电子邮件客户端仅显示发件人标头，而没有任何更多身份验证详细信息。因此，普通用户很难判断邮件的真伪。

此外，某些视觉攻击（例如 A_{12}、A_{13}）无法在协议级别进行防御。一种有效的防御方法是提供用户友好的 UI 通知，并提醒用户他们收到的邮件可能是欺骗邮件。胡等。[20] 还表明，良好的视觉安全通知对于减轻现实世界中的网络钓鱼电子邮件威胁具有积极作用。如图4，部分中的欺骗电子邮件5 可以通过所有三种电子邮件协议进行验证。然而，如果没有 UI 通知，用户无法将此欺骗电子邮件与普通电子邮件区分开来。

如图16，用户可以根据 UI 通知直观地识别收到的电子邮件是否包含恶意行为。国内知名邮件服务商Coremail采纳了我们的建议，在其webmail和邮件客户端实现了UI通知。此外，我们还发布了名为“NoSpoofing”的 Gmail Chrome 扩展形式的 UI 通知方案[1].评估工具。我们已经在 GitHub 上公开发布了我们的测试工具[2] 供电子邮件管理员评估和提高其安全性。配置目标邮件系统信息后，该工具可以与目标系统进行交互，评估目标系统是否容易受到攻击。

7 披露和回应

在这项工作中发现的漏洞已详细报告给所有 30 家相关电子邮件供应商。我们一直在

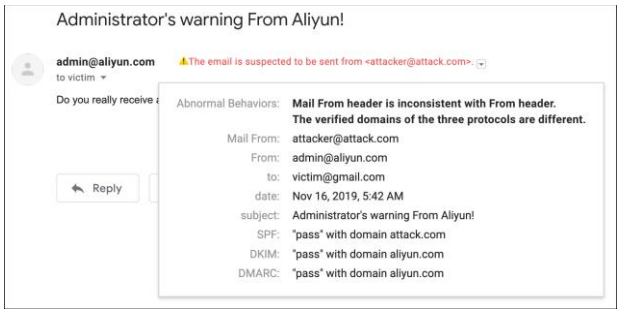


图 16：针对联合攻击的 UI 通知示例

与这些实体接触以帮助他们减轻检测到的威胁。我们的联系结果总结如下。

阿里云：他们对攻击很感兴趣，并与我们就规范进行了深入讨论。他们提到 RFC 6376 建议在电子邮件转发阶段添加 DKIM 签名以提高电子邮件的可信度。他们现在已经认识到在未经验证的情况下添加 DKIM 签名的风险，并承诺评估和修复此类问题。他们还建议我们联系相关 RFC 的作者以达成一致的修复建议。

Gmail：他们承认我们的报告，并将在后续更新中修复相关问题。他们联系我们讨论这些安全问题背后的根本原因。

iCloud：他们与我们讨论了攻击的细节及其潜在后果。特别是Apple iCloud Email，已经通过我们的合作修复了相关的安全问题。

新浪：他们将该问题评估为高危漏洞，并在内部评估相应的防护措施。作为奖励，他们为我们提供了 90 美元的奖励。 ≈

Yandex：他们接受了我们的报告并确认了漏洞。同时，他们提供 200 美元的奖金以表扬。

雅虎：他们确认了漏洞。但他们声称这不是直接的风险。

Coremail：他们承认我们的报告，特别感谢我们报告 UI 攻击问题。为了应对这些安全问题，他们采纳了我们的建议，并开始实施 UI 通知，以保护用户免受电子邮件欺骗攻击。

QQ邮箱和163.com：他们对我们的工作表示赞赏，并通知我们他们将通过反垃圾邮件策略来解决这些安全问题。

Outlook 和 Mail.ru：他们声称他们严格按照 RFC 标准操作他们的电子邮件服务。他们将这些问题归类为钓鱼邮件，并承诺将更加关注此类攻击的影响。

其他：我们已经联系了其他相关的电子邮件供应商，并期待收到他们的反馈。

[1]无欺骗：https://chrome.google.com/webstore/detail/no 欺骗/ehidaopjcnapdglbbbjgeoagpophfjnp

[2]电子邮件欺骗测试工具：https://github.com/mo-xiaoxi/Email 欺骗测试工具

8 相关工作

先前的工作已经揭示了网络钓鱼电子邮件攻击的某些威胁 [8,12]，包括鱼叉式网络钓鱼攻击对电子邮件用户行为的影响[32]. 我们的工作重点是更新颖的欺骗攻击形式及其对整个身份验证过程的影响。 Poddebniak 等人。[37] 讨论实际的欺骗攻击如何破坏 OpenPGP 和 S/MIME 电子邮件签名验证的各种保护。他们还讨论了为增强欺骗检测而提出的两个新协议，例如 BIMI（用于消息识别的品牌指标）[41]和ARC（认证接收链）[3]. 然而，BIMI 建立在 DMARC 之上，尚未完全标准化。因此，我们发现的攻击也是有效的。 ARC 协议于 2019 年标准化，但只有三个供应商（即 Gmail、Office 365、Zoho）在我们的实验目标中部署了该协议。然而，我们的工作发现，Office 365 和 Zoho 都存在 ARC 实施的缺陷，这仍然会导致一些安全问题。

胡等。 [20] 通过端到端的电子邮件欺骗实验分析了电子邮件供应商如何检测和处理欺骗电子邮件。我们发现他们提到的漏洞在过去两年中大部分已经修复。此外，他们没有讨论绕过安全协议检测。我们的工作重点是可以绕过安全协议或用户界面保护的新攻击。我们可以构建一个高度逼真的欺骗电子邮件，它可以完全绕过所有电子邮件安全协议和用户界面保护。

此外，先前的文献已经提出了许多防御传统网络钓鱼攻击的技术。 SPF、DKIM 和 DMARC 等 SMTP 扩展旨在保护电子邮件的真实性。福斯特等人。 [14] 测量了这些协议的实施和部署，并指出，不幸的是，尽管经过多年的发展，这些安全协议的接受率仍然不是很高。这种低接受率严重危及电子邮件生态系统的安全 [19].

此外，还有许多工作讨论了基于从电子邮件内容和标题中提取的特征的网络钓鱼检测方法 [7, 13, 28]，其中很多都依赖于机器学习技术。此外，Ho 等人。 [18] 指出针对网络钓鱼攻击的良好安全指标的积极影响。其他作品[21, 36] 表示当前电子邮件服务没有作为 HTTPS 的 UI 通知 [33]. 当前的视觉安全指标不足以提供全面的网络钓鱼防护 [20, 29]. 对于电子邮件欺骗攻击，我们的研究为电子邮件系统管理员提供了 UI 通知方案和评估工具。它可以有效地促进未来针对电子邮件欺骗的保护措施的发展。

9 结论

本文探讨了电子邮件生态系统中基于链的身份验证结构的漏洞。具体来说，在这种基于链的结构下，任何一个部分的故障都可能破坏整个链条。即，电子邮件的真实性取决于电子邮件身份验证链中最薄弱的环节。通过对电子邮件传递过程的系统分析，我们提出了一系列可以绕过 SPF、DKIM、DMARC 和用户界面保护的新攻击。此外，我们对 30 种流行的电子邮件服务和 23 种电子邮件客户端进行了大规模分析。实验结果表明，所有这些都容易受到新的攻击，包括著名的电子邮件服务，如 Gmail 和 Outlook。我们强调一个不幸的事实，即许多电子邮件服务没有实施足够的保护措施。此外，认识到过去文献的局限性，这些文献侧重于欺骗攻击对身份验证过程的单个步骤的影响， 我们专注于欺骗攻击对基于链的电子邮件认证过程作为一个整体。

根据我们的发现，我们分析了这些攻击的根本原因，并将问题报告给相应的电子邮件服务提供商。我们还为电子邮件协议设计者和电子邮件提供商提出了关键缓解措施，以抵御电子邮件欺骗攻击。我们的工作致力于帮助电子邮件行业更有效地保护用户免受电子邮件欺骗攻击，并提高电子邮件生态系统的整体安全性。

致谢

我们真诚地感谢我们的牧羊人 Zakir Durumeric 和所有匿名审稿人为改进本文所提出的宝贵审阅和意见。我们还感谢 Mingming Zhang、Kangdi Cheng、Zhuo Li、Ennan Zheng 和 Jianjun Chen 的同行评审和协助编辑本文。

这项工作得到了中国国家自然科学基金（批准号 U1836213 和 U1636204）、BNRist 网络和软件安全研究计划（批准号 BNR2019TD01004）的部分支持。

参考文献

[1] 双向文本。 https://en.wikipedia.org/wiki/Bidirectional_text. 访问时间：2019 年 11 月 11 日。

[2] E Allman、Jon Callas、M Delany、Miles Libbey、J Fenton 和 M Thomas。 Domainkeys 识别邮件（dkim）签名。技术报告，RFC 4871，2007 年 5 月。

[3] Kurt Andersen、Brandon Long、S Jones 和 Murray Kucherawy。经过身份验证的接收链（arc）协议。系列Internet-Draft'17，2017。

[4] S 空白和 M Kucherawy。经过身份验证的接收链（arc）协议。 2019.

[5] 恩里科·布兰齐里（Enrico Blanzieri）和安东·布里尔（Anton Bryl）。基于学习的垃圾邮件过滤技术的调查。人工智能评论，29(1):63–92，2008。

[6] Jianjun Chen、Jian Jiang、Haixin Duan、Nicholas Weaver、Tao Wan 和 Vern Paxson。主机问题：http 实现中的多个主机歧义。在 2016 年 ACM SIGSAC 计算机和通信安全会议记录中，第 1516-1527 页。美国计算机学会，2016 年。

[7] Asaf Cidon、Lior Gavish、Itay Bleier、Nadia Korshun、Marco Schweighauser 和 Alexey Tsitkin。高精度检测商业电子邮件泄露。在第 28 届 USENIX 安全研讨会（USENIX 安全 19）中，第 1291–1307 页，2019 年。

[8] Dan Conway、Ronnie Taib、Mitch Harris、Kun Yu、Shlomo Berkovsky 和 Fang Chen。对银行员工信息安全和网络钓鱼体验的定性调查。第十三届可用隐私和安全研讨会（SOUPS 2017），第 115–129 页，2017 年。

[9] D Crocker、T Hansen 和 M Kucherawy。 Domainkeys 识别邮件（dkim）签名（rfc6376）。互联网协会征求意见。（年份：2011 年），2011 年。

[10] 戴夫·克罗克（Dave Crocker）和保罗·奥弗尔（Paul Overell）。语法规范的增强 bnf：Abnf。技术报告，RFC 2234，1997 年 11 月。

[11] Robin Dhamankar、Yoonkyong Lee、AnHai Doan、Alon Halevy 和 Pedro Domingos。 imap：发现数据库模式之间的复杂语义匹配。在 2004 年 ACM SIGMOD 数据管理国际会议记录中，第 383-394 页，2004 年。

[12] 克里斯汀·E·德雷克、乔纳森·J·奥利弗和尤金·J·孔茨。网络钓鱼电子邮件的剖析。在 CEAS 中。引见者，2004 年。

[13] 伊恩·费特、诺曼·萨德和安东尼·托马西奇。学习检测网络钓鱼电子邮件。第 16 届万维网国际会议论文集，第 649-656 页。ACM，2007 年。

[14] Ian D Foster、Jon Larson、Max Masich、Alex C Snoeren、Stefan Savage 和 Kirill Levchenko。任何其他名称的安全性：关于基于提供商的电子邮件安全性的有效性。在第 22 届 ACM SIGSAC 计算机和通信安全会议论文集中，第 450-464 页。美国计算机学会，2015 年。

[15] Ned Freed、Nathaniel Borenstein 等人。多用途互联网邮件扩展（mime）第一部分：互联网邮件正文格式，rfc2045。参见实例*http://ietf. 组织/rfc/rfc2045。文本文件，1996 年。*

[16] Evgeniy Gabrilovich 和 Alex Gontmakher。同形异义词攻击。 ACM 通讯，45(2):128，2002。

[17] Markus Gruber、Phillip Wieser、Stefan Nachtnebel、Christian Schanes 和 Thomas Grechenig。从 rfcs 中提取 abnf 规则以实现自动化测试数据生成。在 IFIP 国际信息安全会议上，第 111-124 页。施普林格，2013 年。

[18] Grant Ho、Aashish Sharma、Mobin Javed、Vern Paxson 和 David Wagner。检测企业设置中的凭据鱼叉式网络钓鱼。第 26 届 USENIX 安全研讨会（USENIX 安全 17），第 469–485 页，2017 年。

[19] 航虎、彭彭和王刚。了解在电子邮件系统中采用反欺骗协议。 2018 年 IEEE 网络安全发展（SecDev），第 94-101 页。 IEEE，2018 年。

[20] 杭虎和王刚。电子邮件欺骗攻击的端到端测量。在第 27 届 USENIX 安全研讨会（USENIX 安全 18）中，第 1095-1112 页，2018 年。

[21] 杭虎和王刚。重新审视电子邮件欺骗攻击。 arXiv 预印本 arXiv:1801.00853，2018。

[22] Tom N Jagatic、Nathaniel A Johnson、Markus Jakobsson 和 Filippo Menczer。社交网络钓鱼。 ACM 通讯，50(10):94–100，2007。

[23] 斯科特·基特曼。 Rfc 7208 – 用于授权在电子邮件中使用域的发件人策略框架（spf），第 1 版，2014 年。

[24] 斯科特·基特曼。用于授权在电子邮件中使用域的发件人策略框架（spf），版本 1。2014 年。

[25] *J克伦辛。简单邮件传输协议（rfc5321）。网络工作组，互联网工程任务组。 http://tools. ietf. 组织/html/rfc5321，2008 年。*

[26] 约翰·克伦辛。 Rfc 2821：简单邮件传输协议。*征求意见，网络工作组，2001 年。*

[27] John Klensin、Randy Catoe 和 Paul Krumviede。Imap/pop 授权扩展用于简单的质询/响应。在 RFC 2195 中。网络工作组，1997 年。

[28] 蒂姆·克劳斯 (Tim Krause)、拉斐尔·尤茨 (Rafael Uetz) 和蒂姆·克莱舒曼 (Tim Kretschmann)。仅从元数据中识别垃圾邮件。 2019 年 IEEE 通信和网络安全会议 (CNS)，第 178-186 页。 IEEE，2019 年。

[29] Kat Krol、Matthew Moroz 和 M Angela Sasse。不工作。不能工作？为什么是时候重新考虑安全警告了。 2012 年第七届互联网和系统风险与安全国际会议 (CRiSIS)，第 1-8 页。 IEEE，2012 年。

[30] M库切拉维。 Domainkeys 识别邮件 (dkim) 和邮件列表。技术报告，RFC 6377，2011 年 9 月。

[31] Murray Kucherawy 和 Elizabeth Zwicky。基于域的消息身份验证、报告和一致性 (dmarc)。 2015.

[32] Tian Lin、Daniel E Capecci、Donovan M Ellis、Harold A Rocha、Sandeep Dommaraju、Daniela S Oliveira 和 Natalie C Ebner。鱼叉式网络钓鱼电子邮件的易感性：互联网用户人口统计和电子邮件内容的影响。 ACM 人机交互交易 (TOCHI)，26(5):32，2019 年。

[33] Meng Luo、Oleksii Starov、Nima Honarmand 和 Nick Nikiforakis。后见之明：了解移动浏览器中 ui 漏洞的演变。在 2017 年 ACM SIGSAC 计算机和通信安全会议记录中，第 149-162 页。美国计算机学会，2017 年。

[34] 域名密钥识别邮件。签名 rfc 6376。

[35] 约书亚佩雷达。 boofuzz：人类网络协议模糊测试。访问时间：2017 年 2 月 17 日。

[36] Justin Petelka、Yixin Zou 和 Florian Schaub。将警告放在链接所在的位置：改进和评估电子邮件网络钓鱼警告。在 2019 年 CHI 计算系统人为因素会议论文集中，第 518 页。ACM，2019 年。

[37] Damian Poddebniak、Christian Dresen、Jens Müller、Fabian Ising、Sebastian Schinzel、Simon Friedberger、Juraj Somorovsky 和 Jörg Schwenk。Efail：使用渗漏通道破解 s/mime 和 openpgp 电子邮件加密。第 27 届 {USENIX} 安全研讨会 ({USENIX} 安全 18)，第 549–566 页，2018 年。

[38] 乔恩·波斯特尔。简单的邮件传输协议。信息科学，1982。

[39] 保罗·雷斯尼克。 Rfc2822：互联网消息格式，2001。

[40] 保罗·雷斯尼克。 Rfc 5322，互联网消息格式。在线：https://tools. ietf.组织/html/rfc5322，2008 年。

[41] T. Loder S. Blank、P. Goldstein 和 T. Zink。消息识别 (bimi) 的品牌指标。技术报告，2019 年。