清華大學
Tsinghua University

An Introduction to Email Security

清华大学网络科学与网络空间研究院

王楚涵
wch22@mails.tsinghua.edu.cn

Introduction

《黑神话：悟空》交流活动

关于报名参加《黑神话：悟空》交流活动的通知

发起会议

2024-10-12 22:37:44

发件人： "3A游戏协会"<game@tsginhua.cn>

收件人： "Chuhan Wang"<wch22@mails.tsinghua.edu.cn>

各位同学：

为了感谢各位玩家的支持，本协会将于2024年10月19日（星期六）晚7:00-9:00邀请《黑神话：悟空》主创团队来校交流。现场准备300份系列周边，包括：悟空手办模型、天命人T恤和天命人马克杯等礼物。

请感兴趣的同学于10月15日23：00之前点击下方链接完成报名登记，名额有限，先到先得。报名成功后，活动详细信息将通过短信或邮件通知。

报名地址：https://game.tsinghua.edu.cn

清华大学3A游戏协会

2024年10月12日

《黑神话：悟空》交流活动

关于报名参加《黑神话：悟空》交流活动的通知

发件人： "3A游戏协会"<game@tsginhua.cn>

收件人： "Chuhan Wang"<wch22@mails.tsinghua.edu.cn>

各位同学：

为了感谢各位玩家的支持，本协会将于2024年10月19日（星期六）晚7:00-9:00邀请《黑神话：悟空》主创团队来校交流。现场准备300份系列周边，包括：悟空手办模型、天命人T恤和天命人马克杯等礼物。

请感兴趣的同学于10月15日23：00之前点击下方链接完成报名登记，名额有限，先到先得。报名成功后，活动详细信息将通过短信或邮件通知。

报名地址：https://game.tsinghua.edu.cn

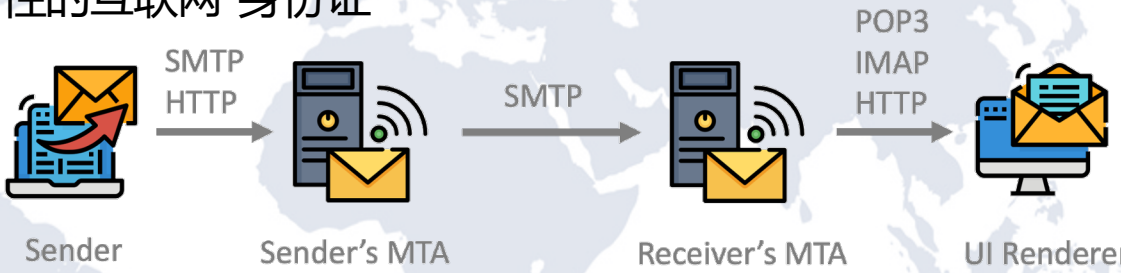
清华大学3A游戏协会

2024年10月12日

电子邮件系统

➢ 互联网基础性的应用系统

- ❖ 学术交流和商业合作的重要通信工具
- ❖ 全球最通用的互联网应用之一
- ❖ 具有唯一性的互联网“身份证”

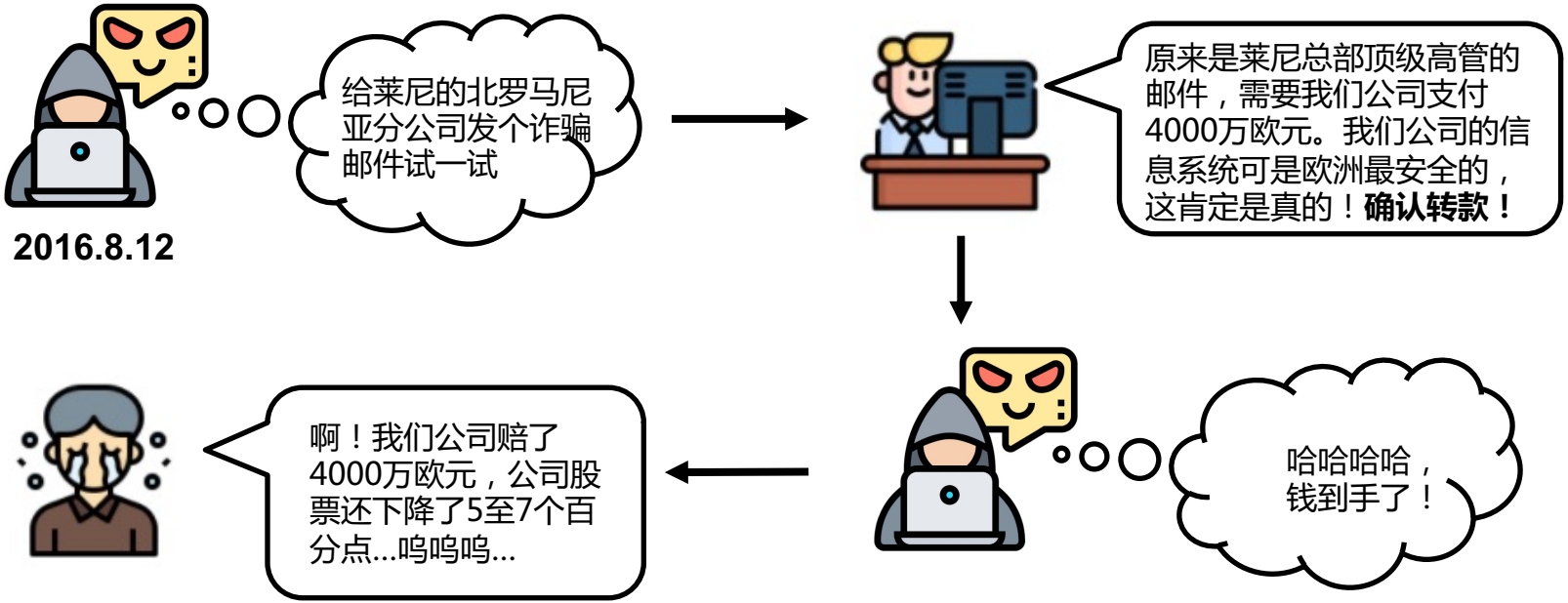


➢ 互联网上“最古老”的应用

- ❖ 1982年，SMTP首次作为互联网标准被写进了RFC文档
- ❖ SMTP作为基础协议已使用发展40余年
- ❖ 协议基本框架至今无明显改变

邮件服务是网络攻击的重要目标

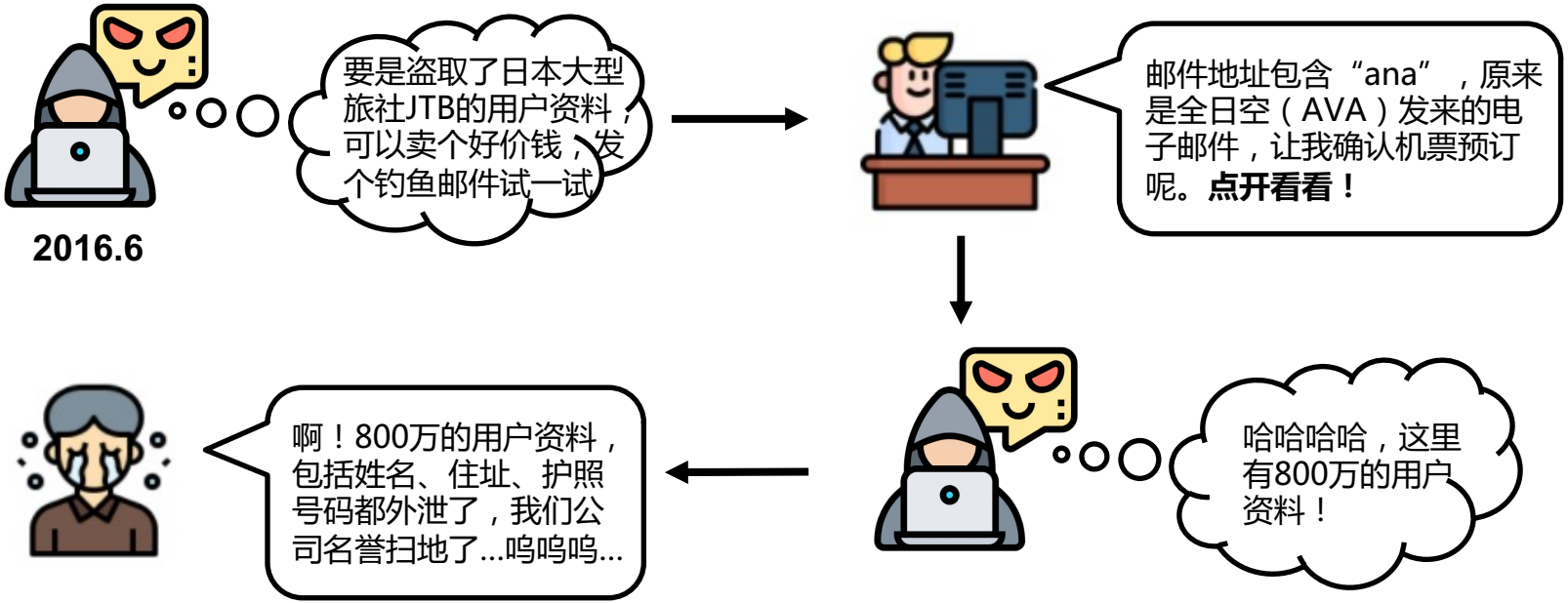
商业电子邮件欺诈（BEC）—— 德国莱尼集团遭邮件诈骗 直接损失4000万欧元



德国莱尼集团遭邮件诈骗 4000 万欧元

邮件服务是网络攻击的重要目标

作为病毒、木马和勒索软件的载体 —— 带毒邮件盗取日大型旅社800万用户资料



带毒邮件盗取日大型旅社 800 万用户资料

希拉里邮件门事件

希拉里团队的竞选主席约翰·波德斯塔收到一封看似来自Google的警告邮件称，有人试图侵入他的账号，需要立即更改邮箱密码。波德斯塔的助手将警告邮件转给技术人员后，得到回复：“这是一封合法邮件”。

随后，波德斯塔的助手放心点开邮件中的钓鱼链接，将波德斯塔近十年来的6000余封邮件拱手送给了黑客。

From: Google <no-reply@accounts.googlemail.com>
Date: March 19, 2016 at 4:34:30 AM EDT
To: john.podesta@gmail.com
Subject: Someone has your password

Someone has your password

Hi John

Someone just used your password to try to sign in to your Google Account john.podesta@gmail.com.

Details:
Saturday, 19 March, 8:34:30 UTC
IP Address: 134.249.139.239
Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

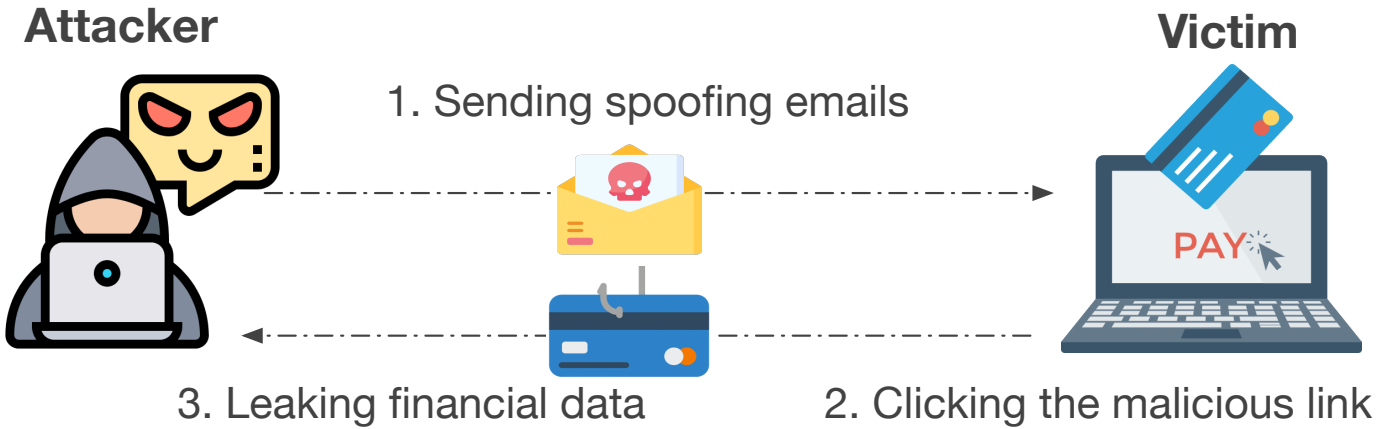
CHANGE PASSWORD

Best,
The Gmail Team

http://www.sic.gov.cn/News/91/7894.htm

邮件伪造攻击

- 邮件伪造攻击技术是一种重要的邮件攻击方法，通过伪造发信人身份来获得受害者信任，进而实现攻击者下一步的目标。



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.

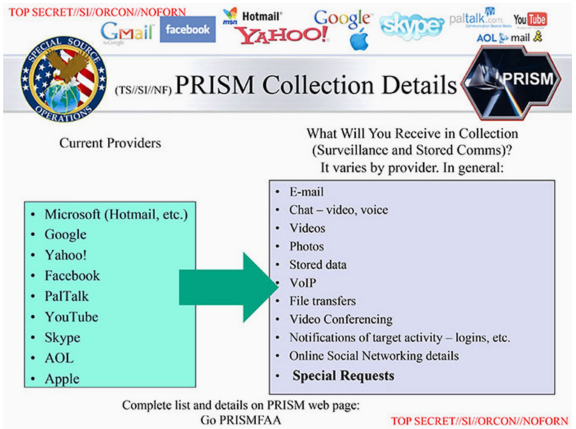
邮件服务是网络攻击的重要目标

➢ 中间人攻击（MITM）

- ❖ SMTP协议设计之初是一个明文传输的网络协议，所以很容易遭受中间人攻击。
- ❖ 攻击者可以通过监控网络流量来直接获取邮件的明文内容。

➢ 斯诺登“棱镜门”事件

- ❖ 2013年，斯诺登通过《华盛顿邮报》曝光了美国国家安全局和联邦调查局的“棱镜计划”。该计划可以让政府部门直接监控用户的电子邮件内容、即时聊天记录、视频、文件等敏感数据。



邮件服务是网络攻击的重要目标

针对国内目标的邮件钓鱼攻击屡见不鲜、危害严重。多家互联网公司曾经中招。

➢ 2022.5 搜狐员工邮箱收到诈骗邮件

https://www.sohu.com › ... · Translate this page

搜狐：部分员工邮箱收到诈骗邮件24名员工被骗4万余元

21 hours ago — 新京报贝壳财经讯（记者宋美璐） 5月25日下午，搜狐官方微博发表声明称：5月18日凌晨，搜狐部分员工邮箱收到诈骗邮件。经调查，实为某员工使用邮件时 ...

https://finance.sina.com.cn › tech › d... · Translate this page

搜狐全体员工遭遇“工资补助”诈骗损失惨重，企业邮箱服务安全 ...

1 day ago — 数据显示，90%的黑客攻击都是通过邮箱作为突破口的，电子邮箱直接关系着企业安全。 回到搜狐邮件诈骗事件，可疑邮件发信地址为sohutv-legal@sohu-inc.com ...

➢ 2022.2 B站企业邮箱遭受钓鱼攻击

https://cn-sec.com › archives · Translate this page

B站企业邮箱发全员钓鱼链接致多员工被骗达8万元公司被质疑 ...

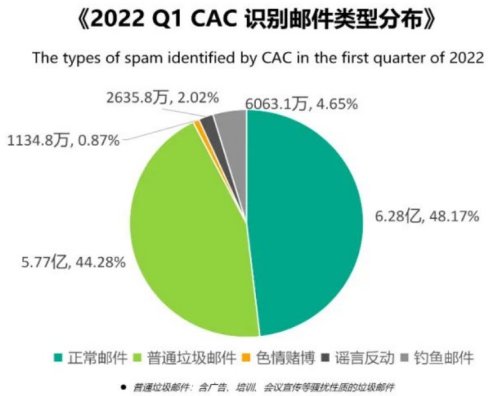
9 Feb 2022 — 而从该微博内容附件的图片显示，受害员工成立了“钓鱼邮件受害者”群，目前群内有72人，有B站受骗员工咨询相关部门HRBP得到的回复是，建议同事自行报警。群 ...

https://www.secrss.com › articles · Translate this page

B站企业邮箱发全员钓鱼链接致多员工被骗达8万元 - 安全内参

9 Feb 2022 — 炯燃科技2月7日讯（安琪）2月7日晚间，发布B站员工猝死消息的微博博主王落北继续爆料，称B站公司内部邮件存在钓鱼链接，致员工受骗金额达8万元。

Missing: 事件 | Must include: 事件



数据来源：CAC邮件安全大数据中心

Coremail | 邮件安全

发生在我们周围的钓鱼攻击

发生在我们周围的钓鱼攻击

关于开展2021年电子身份年审工作的通知 发起会议 精简信息

发件人： notice@tsinghua.edu.cn

时　间： 2021年11月24日 13:48:15 (星期三)

收件人： yang-r20@mails.tsinghua.edu.cn shw18@mails.tsinghua.edu.cn gml18@mails.tsinghua.edu.cn wang-ch19@mails.tsinghua.edu.cn liusy18@mails.tsinghua.edu.cn ...[↓还有5个联系人]

关于开展2021年电子身份年审工作的通知

为保障师生的密码安全，学校决定自11月24日中午12时起开展2021年度电子身份年审工作，现就具体工作通知如下：

一、年审时间：2021年11月24日中午12时至12月1日中午12时

二、年审范围：电子身份全体用户（不包含离退休人员）

三、年审要求：

11月24日中午12时至12月1日中午12时，用户需**及时登录学校用户电子身份服务系统（https://id.tsinghua.edu.cn）确认密码状态**，查询密码修改历史。

密码状态为建议修改的用户请及时修改密码，以免影响信息门户、电子邮箱的访问。密码状态正常的用户可以选择保留原密码继续使用，建议定期修改密码。

四、特别提示：

用户电子身份认证系统具备绑定手机找回密码功能，建议用户在修改个人密码的同时绑定手机号。

说明：清华大学电子身份是指个人证件号+账号+密码的统称。个人证件号包括学号、工作证号、校园卡号等人员编号，账号包括网络连接账号、电子邮箱账号。使用清华大学电子身份登录可以访问并使用校园网、电子邮件、信息门户、网络学堂、图书馆以及学校认可的其他校园网络信息服务资源。

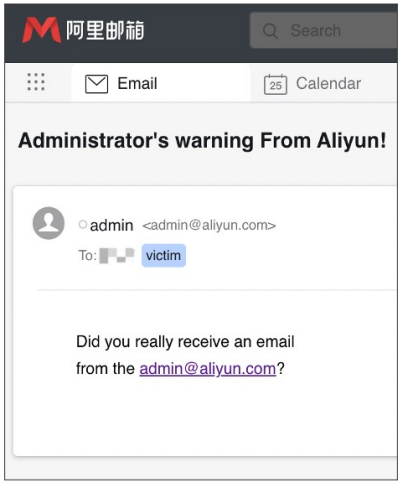
咨询电话：62784859

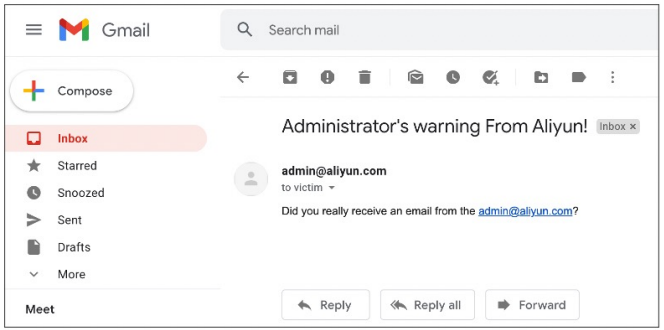
特此通知。

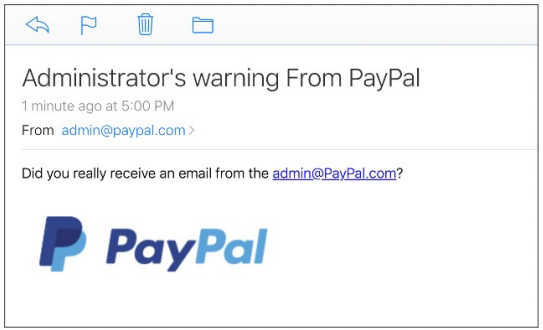
信息化工作办公室

大量的邮件服务受到影响

Gmail
YAHOO! MAIL
163 网易免费邮 mail.163.com
Coremail
Outlook
Yandex Mail
QQ邮箱 mail.qq.com
FOXMAIL
mail.ru group
Apple Mail
阿里邮箱







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

Background

邮件基础协议

SMTP协议

SMTP(Simple Mail Transfer Protocol) 即简单邮件传输协议，是整个邮件传输体系中最基础的框架协议。1982年，SMTP协议首次作为互联网标准被写进了RFC文档，此后被数次更新，最近一次比较大的更新是2008年，更新的标准文档为RFC5321。

身份认证：SMTP 登陆

C: ehlo anonymous.local\r\n
S: 250 ok
C: AUTH PLAIN
AHNrdzIwQG1haWxzLnRzaW…==\r\n
S: 235 Authentication successful\r\n
C: MAIL FROM:
<user1@mails.tsinghua.edu.cn>\r\n
S: 250 Mail OK\r\n
C: rcpt TO:<nislemail@163.com>\r\n
S: 250 Mail OK\r\n

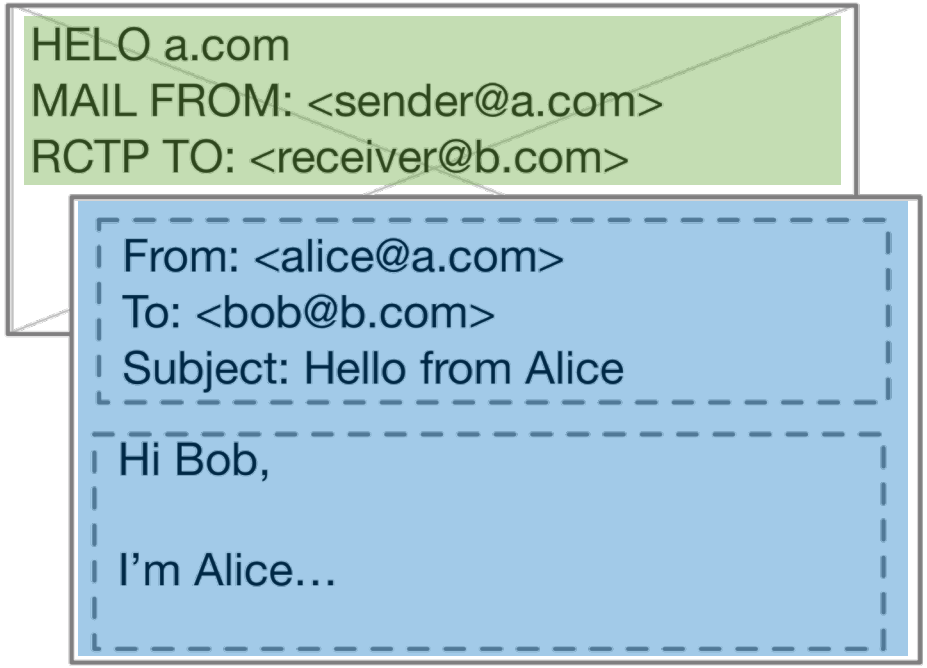
SMTP 发信：路由信息

C: From: ”Admin" <user1@mails.tsinghua.edu.cn>
C: To: ”Admin " <admin@mails.tsinghua.edu.cn >
C: Date: Tue, 15 Jan 2021 16:02:43 -0500
C: Subject: Test message
C:
C: Hello Admin.
C: This is a test message with 5 header fields and 4 lines in the message body.
C: Your friend,
C: user1
C: .
S: 250 Ok: queued as 12345
C: QUIT
S: 221 Bye
{The server closes the connection}

SMTP 发信：邮件信息

SMTP协议

SMTP(Simple Mail Transfer Protocol) 即简单邮件传输协议，是整个邮件传输体系中最基础的框架协议。1982年，SMTP协议首次作为互联网标准被写进了RFC文档，此后被数次更新，最近一次比较大的更新是2008年，更新的标准文档为RFC5321。



SMTP Envelope

普通用户不可见

Message Header

显示在UI界面上

Message Body

POP3/IMAP

- **POP3(Post Office Protocol 3),** 即邮局协议， 负责从邮件服务器中检索电子邮件，于1984年由RFC 937首次定义，并于2007年由RFC 5034更新。
- **IMAP (Internet Message Access Protocol)** ， 即互联网信息访问协议，是另一种广泛用于邮件客户端与服务器之间的协议，由RFC 3501 定义。
- **区别：**
  - IMAP 协议提供邮件客户端与邮件服务器之间的双向通信，客户端的操作将反馈给服务器；POP3仅为单向通信，客户端上的操作（如移动电子邮件，标记为已读等）不会反馈到服务器；
  - IMAP协议允许多个邮件客户端同时访问与加载；POP协议要求当前连接的客户端是唯一邮件客户端；

POP3/IMAP

❖ POP3(Post Office Protocol 3)

```
S: <wait for connection on TCP port 110>
C: <open connection>
S:    +OK POP3 server ready <1896.697170952@dbc.mtview.ca.us>
C:    APOP mrose c4c9334bac560ecc979e58001b3e22fb
S:    +OK mrose's maildrop has 2 messages (320 octets)
C:    STAT
S:    +OK 2 320
C:    LIST
S:    +OK 2 messages (320 octets)
S:    1 120
S:    2 200
S:    .
C:    RETR 1
S:    +OK 120 octets
S:    <the POP3 server sends message 1>
S:    .
C:    DELE 1
S:    +OK message 1 deleted
C:    RETR 2
S:    +OK 200 octets
S:    <the POP3 server sends message 2>
S:    .
C:    DELE 2
S:    +OK message 2 deleted
C:    QUIT
S:    +OK dewey POP3 server signing off (maildrop empty)
C: <close connection>
S: <wait for next connection>
```

❖ IMAP(Internet Message Access Protocol)

```
C: <open connection>
S:   * OK IMAP4rev1 Service Ready
C:   a001 login mrc secret
S:   a001 OK LOGIN completed
C:   a002 select inbox
S:   * 18 EXISTS
S:   * FLAGS (\Answered \Flagged \Deleted \Seen \Draft)
S:   * 2 RECENT
S:   * OK [UNSEEN 17] Message 17 is the first unseen message
S:   * OK [UIDVALIDITY 3857529045] UIDs valid
S:   a002 OK [READ-WRITE] SELECT completed
C:   a003 fetch 12 full
S:   * 12 FETCH (FLAGS (\Seen) INTERNALDATE "17-Jul-1996 02:44:25 -0700"
      RFC822.SIZE 4286 ENVELOPE ("Wed, 17 Jul 1996 02:23:25 -0700 (PDT)"
      "IMAP4rev1 WG mtg summary and minutes"
      (("Terry Gray" NIL "gray" "cac.washington.edu"))
      (("Terry Gray" NIL "gray" "cac.washington.edu"))
      (("Terry Gray" NIL "gray" "cac.washington.edu"))
      ((NIL NIL "imap" "cac.washington.edu"))
      ((NIL NIL "minutes" "CNRI.Reston.VA.US")
      ("John Klensin" NIL "KLENSIN" "MIT.EDU")) NIL NIL
      "<B27397-0100000@cac.washington.edu>")
      BODY ("TEXT" "PLAIN" ("CHARSET" "US-ASCII") NIL NIL "7BIT" 3028
      92))
S:   a003 OK FETCH completed
C:   a004 fetch 12 body[header]
```

邮件协议的演进

MIME协议

1992年MIME协议诞生，从此邮件可以传输任意二进制数据。

端到端加密

20世纪90年代，PGP与S/MIME协议相继诞生，用于对邮件内容进行端到端的加密。

斯诺登棱镜门

废弃明文传输

RFC 8314 明确建议不要在邮件传输中使用明文，建议使用implicit TLS。

邮件基础协议

20世纪80年代，SMTP、POP、IMAP三大邮件基础协议诞生

STARTTLS

1999年STARTTLS诞生，三大邮件基础协议打上了SSL/TLS补丁。

身份认证协议

21世纪以来，SPF、DKIM、DMARC被相继提出，用于验证发信人的身份。

希拉里邮件门

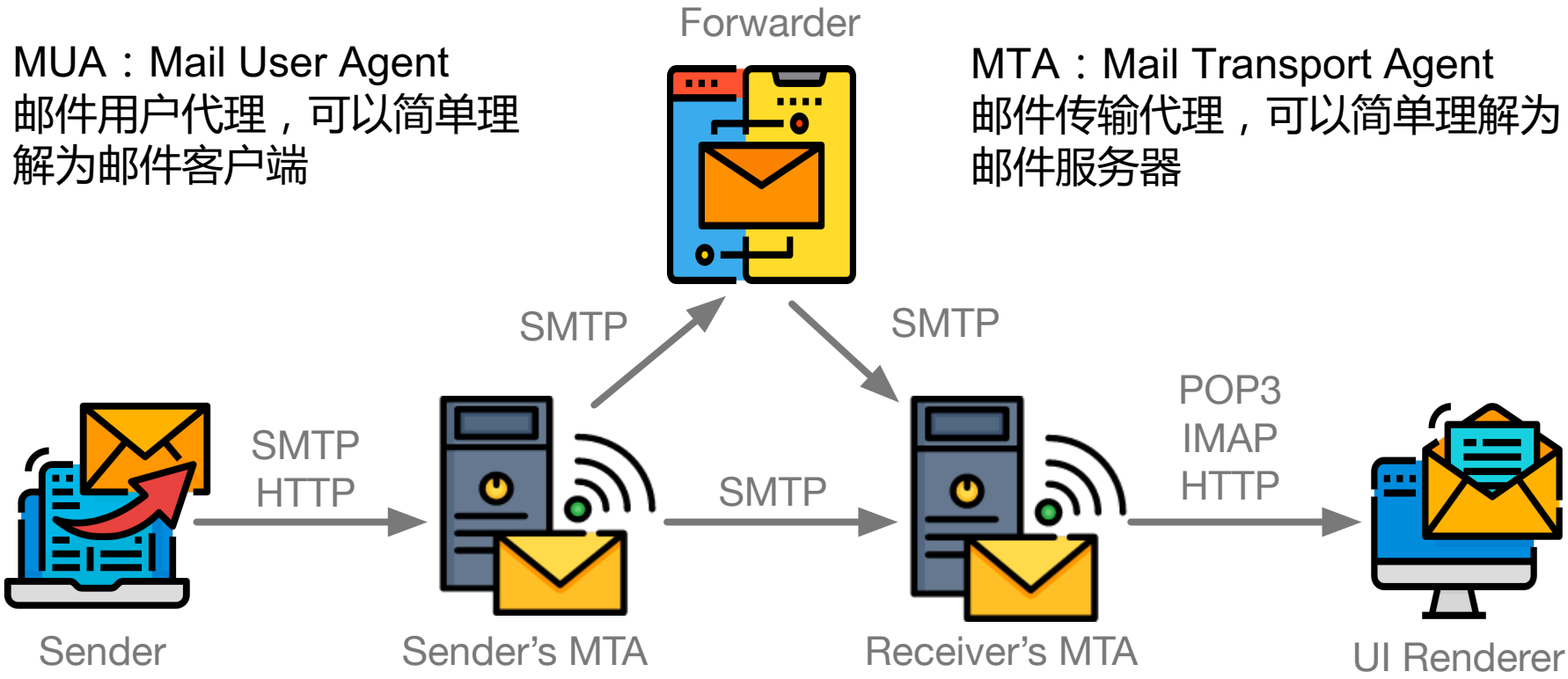
新兴协议

邮件协议依旧在不断演进着，新兴的邮件协议依旧在不断的诞生DANE、MTA-STS、ARC...

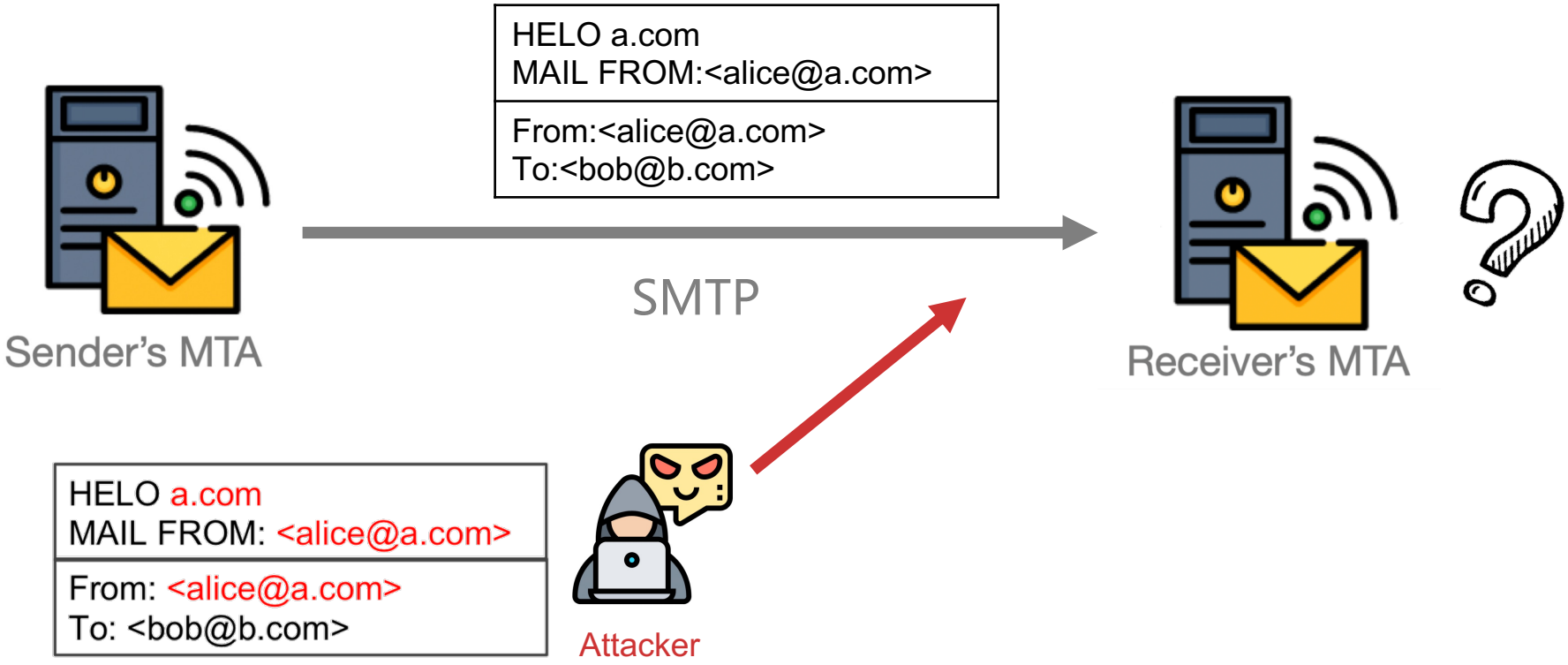
邮件传输过程

MUA：Mail User Agent
邮件用户代理，可以简单理解为邮件客户端

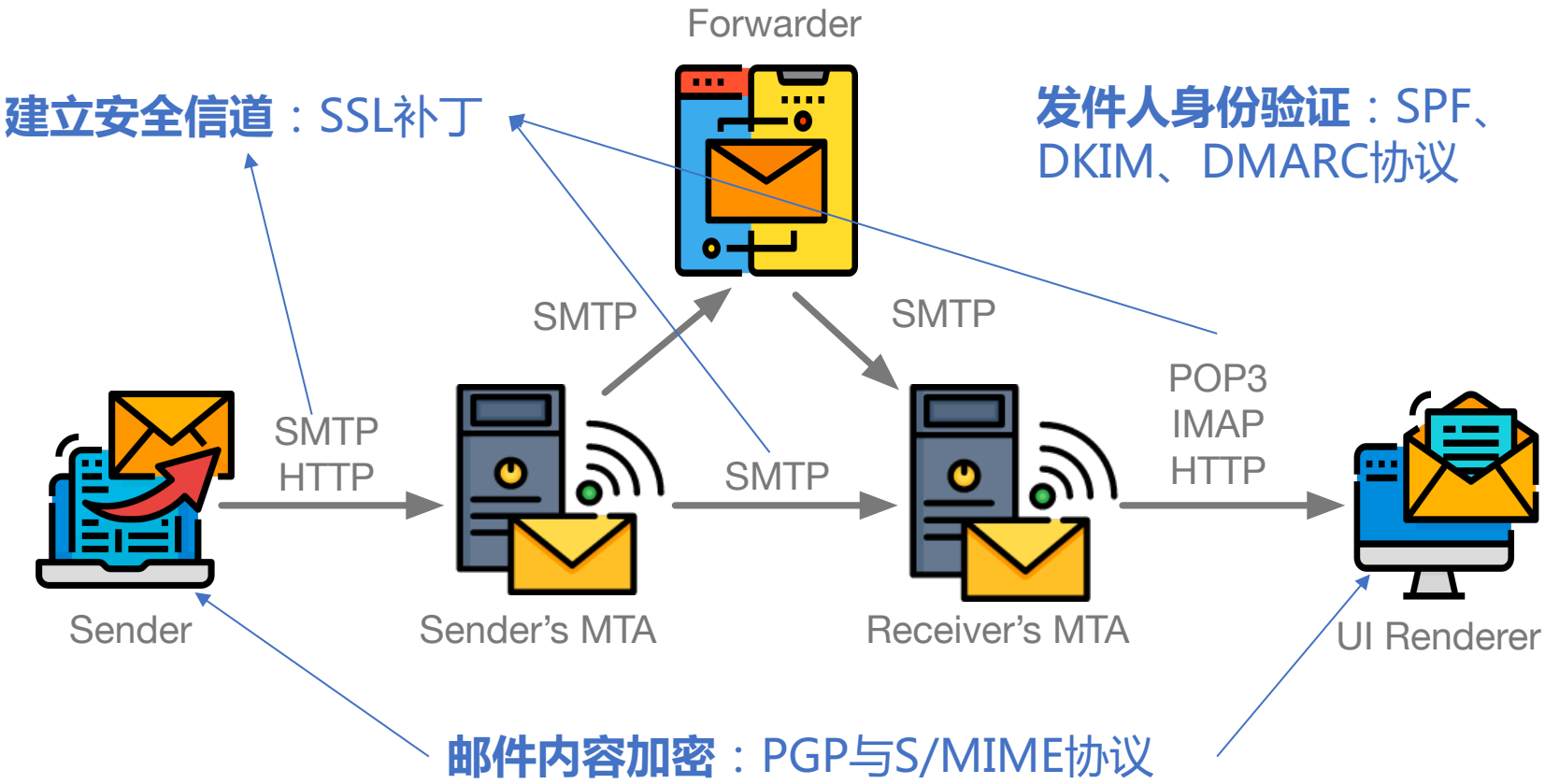
MTA：Mail Transport Agent
邮件传输代理，可以简单理解为邮件服务器



SMTP协议缺少必要的身份验证机制



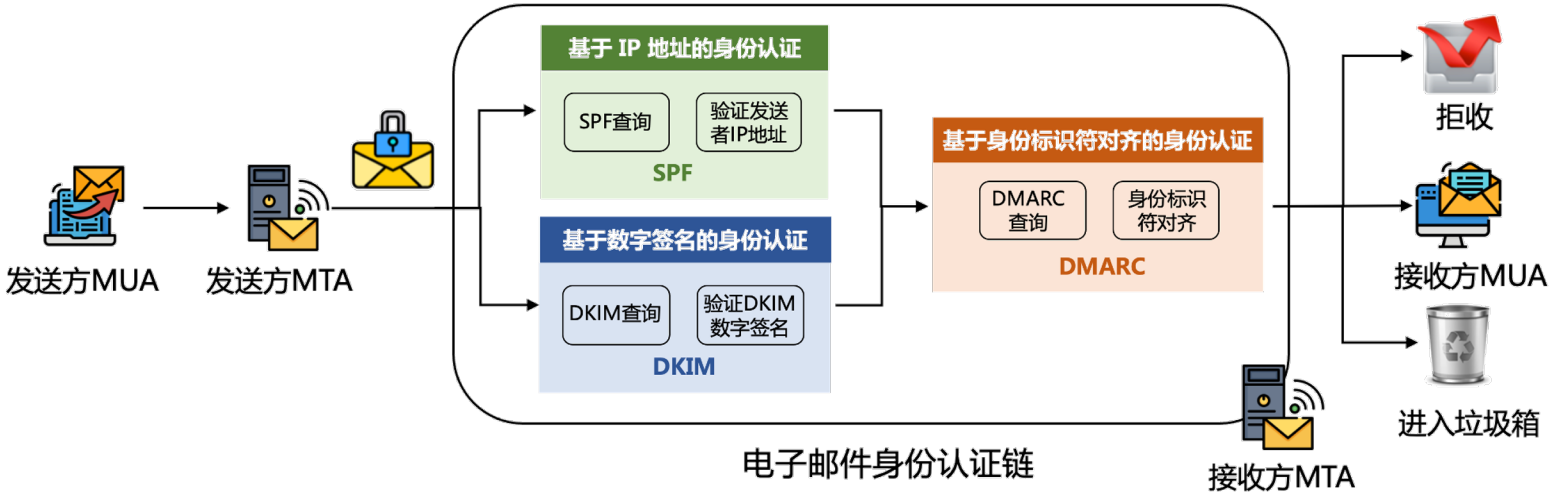
邮件安全拓展协议


Forwarder
建立安全信道：SSL补丁
发件人身份验证：SPF、DKIM、DMARC协议
SMTP
SMTP
SMTP
HTTP
SMTP
POP3
IMAP
HTTP
Sender
Sender's MTA
Receiver's MTA
UI Renderer
邮件内容加密：PGP与S/MIME协议

邮件身份认证协议

邮件身份认证协议

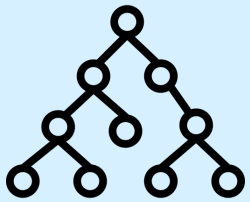
协议名称	RFC文档	工作机制
SPF	RFC 7208	基于MAIL FROM/HELO中的信息验证**发送方的IP地址**
DKIM	RFC 6376	通过添加**数字签名**的方式实现邮件内容完整性的保护
DMARC	RFC 7489	基于SPF/DKIM的验证结果，将上述协议验证的身份与MIME From比对。（**身份标识符对齐**）



SPF协议

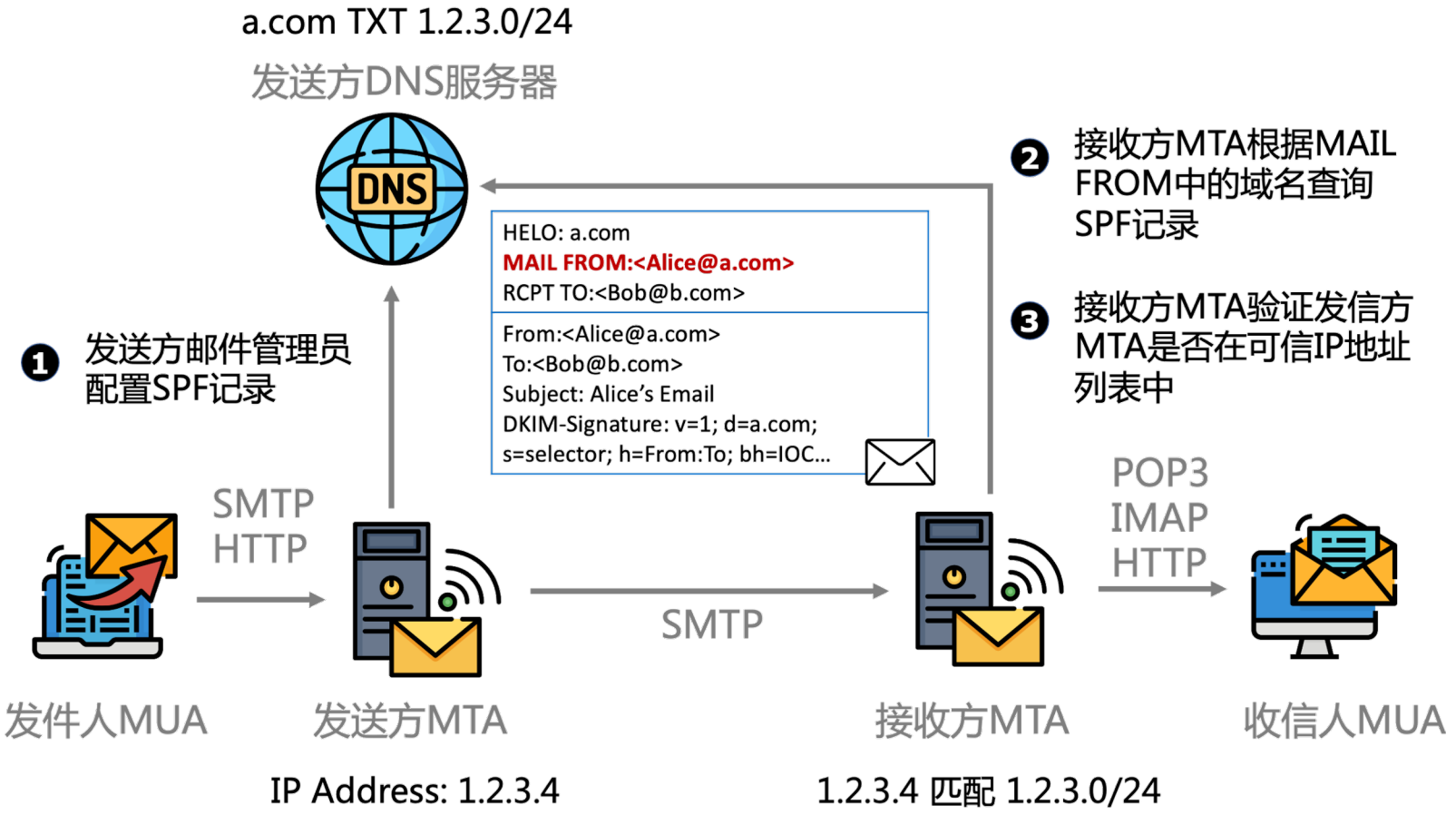
- **发件人策略框架(Sender Policy Framework，SPF)**
  - SPF 是一种**基于 IP 地址的电子邮件身份认证协议**。SPF 通过验证邮件传输代理 (MTA) 的 IP 地址来验证发信人身份。
  - 电子邮件管理员在域名系统（DNS）中的TXT记录中添加 SPF 记录，列出**有权代表该域发送邮件的IP地址列表**。
  - 收件方通过查询发送方域名对应的SPF记录，并与真实发信 IP 地址判断邮件的真实性。

```
→ dig txt +short tsinghua.edu.cn
"v=spf1 redirect=spf.tsinghua.edu.cn”

→ dig txt +short spf.tsinghua.edu.cn
"v=spf1 ip4:101.6.4.0/24 ip4:166.111.204.0/24 ip4:183.172.3.24/29
ip4:183.173.3.24/29 include:spf.icoremail.net -all”
```



SPF依赖树

SPF验证流程


a.com TXT 1.2.3.0/24
发送方DNS服务器
DNS
1 发送方邮件管理员配置SPF记录
2 接收方MTA根据MAIL FROM中的域名查询SPF记录
3 接收方MTA验证发信方MTA是否在可信IP地址列表中
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
DKIM-Signature: v=1; d=a.com;
s=selector; h=From:To; bh=IOC...
SMTP
HTTP
SMTP
POP3
IMAP
HTTP
发件人MUA
发送方MTA
接收方MTA
收信人MUA
IP Address: 1.2.3.4
1.2.3.4 匹配 1.2.3.0/24

DKIM协议

- **域名密钥识别邮件标准(DomainKeys Identified Mail，DKIM)**
  - DKIM是一种基于**数字签名**的身份验证协议。DKIM 协议会对电子邮件添加数字签名，来保护邮件内容的**完整性**和**真实性**。
  - DKIM签名基于哈希算法和非对称加密算法（RSA）生成。
  - DKIM的公钥会部署在一个格式如下的域名上：

<selector>._domainkey.*<example.com>*

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
s=selector; d=example.com; h=From:To:Subject; l=200;
bh=vYFvy46eesudgj4s…; b=IHEFQ+7rcisqsRBSEdd83…

An Example of DKIM Signature Header.

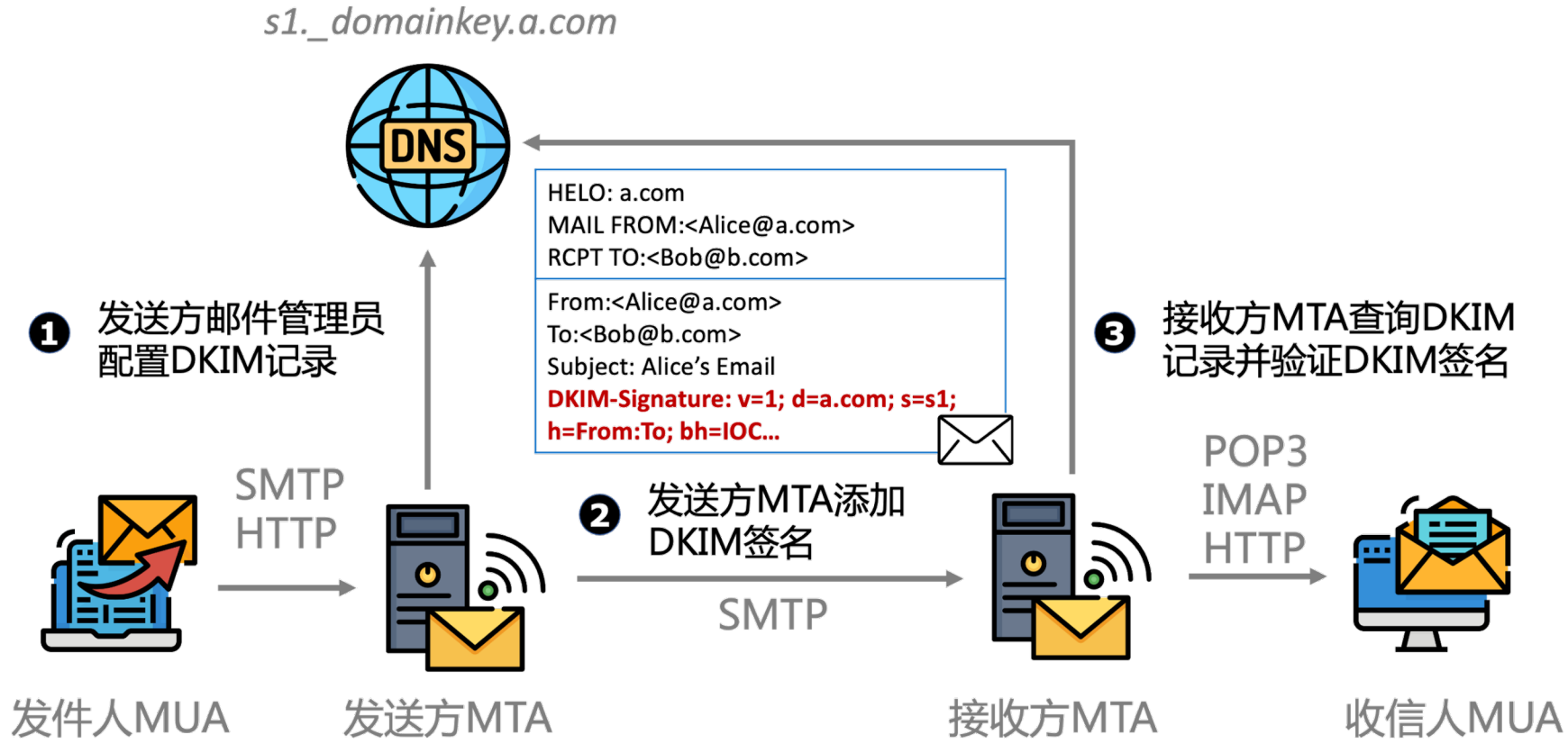
DKIM签名

1. d字段　记录签发者的域名，也是DKIM签名验证的身份实体
2. s字段　签发者选择的selector，一个随机的字符串
3. h字段　记录DKIM签名保护的邮件头字段
4. l字段　记录被DKIM签名保护的正文范围（字节数）
5. bh字段 邮件正文部分的哈希值
6. b字段　包含用h标签给出的头字段，以及DKIM签名头字段本身，计算签名时会先将b标记自身的值视为空字符串。签名因为包含了bh标签，所以间接覆盖了邮件正文。

DKIM-Signature: v=1; a=rsa-sha1; c=relaxed/relaxed; d=quora.com; h=content-type:mime-version:from:to:subject:list-unsubscribe:date:message-id; s=pigeon; bh=nsj8O2OEdQa8f9VPv4vALOeo7iY=; b=PXPOwn8QFuW8bxxnFAzlPyP3DVdTsgUopsMk2mlsu7/kzsrTmVRnYqKn8ZsRmHyWMhzxoJ Ptb+aQYhkasfo/bj7jaHj9hz30crhTVUDBJYWf0bVm6/qn2Ux16LwHyREVn+j5Vj mOWSNOLWWypUPx6D1FlRbGnWTyGWh5zgStF23oAimGJ4DFiB2Pq2lk9J6/Kio6jg b78xxBKHPgeArT6SqqTUx7HE1HBSKQYKAOYoG5XLxMtSn2tUMMwmyORsOj4ChAiV 3aZkbhCzN+yEqNBy3vD/ycuMfgFmThgIKc1GXqCOgQ1W4a/wlckrbZtVAlSJSWy1 CNo27Nj5QlEVwnIA==

一个真实的DKIM签名

DKIM验证流程


s1._domainkey.a.com
DNS
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
DKIM-Signature: v=1; d=a.com; s=s1;
h=From:To; bh=IOC...
1 发送方邮件管理员
配置DKIM记录
2 发送方MTA添加
DKIM签名
3 接收方MTA查询DKIM
记录并验证DKIM签名
SMTP
HTTP
SMTP
POP3
IMAP
HTTP
发件人MUA
发送方MTA
接收方MTA
收信人MUA

DMARC协议

DMARC是构建在 SPF 和 DKIM 验证结果之上的验证协议。

DMARC协议主要解决了SPF/DKIM没能完全解决的三个问题：

① 用户在前端界面看到的发信人信息是MIME From字段，而SPF和DKIM保护的身份实体都不是MIME From字段，DMARC增加了身份对齐的过程

② DMARC 允许域管理所有者发布一个策略，以指定当传入的电子邮件未能通过 SPF 和 DKIM 检查时，接收者应该采取什么操作。

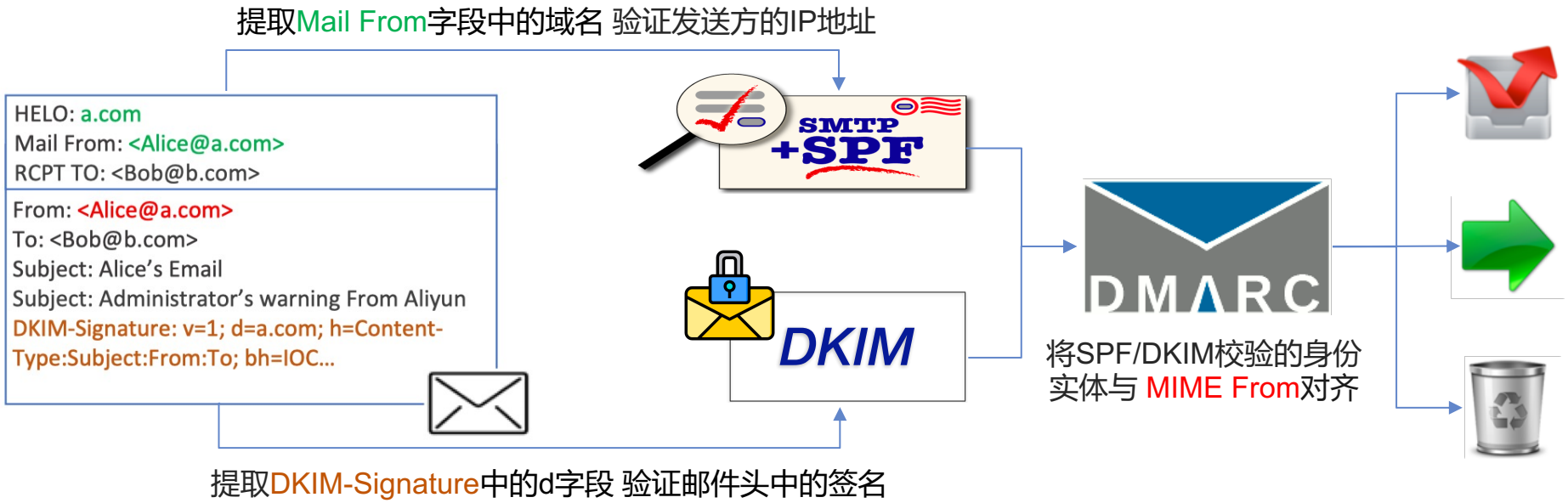
③ DMARC 会定期将验证失败的邮件反馈给DMARC的部署方，帮助部署方修正协议部署

邮件服务的 DMARC 记录通常部署在一个指定的域名TXT记录中：

_dmarc.*<example.com>*

"v=DMARC1; p=none; fo=1; ruf=mailto:dmarc@mail.tsinghua.edu.cn; rua=mailto:dmarc_report@mail.tsinghua.edu.cn"

DMARC验证流程



DMARC协议验证通过的前提条件：

（1）SPF与DKIM协议其中之一验证通过 或的关系

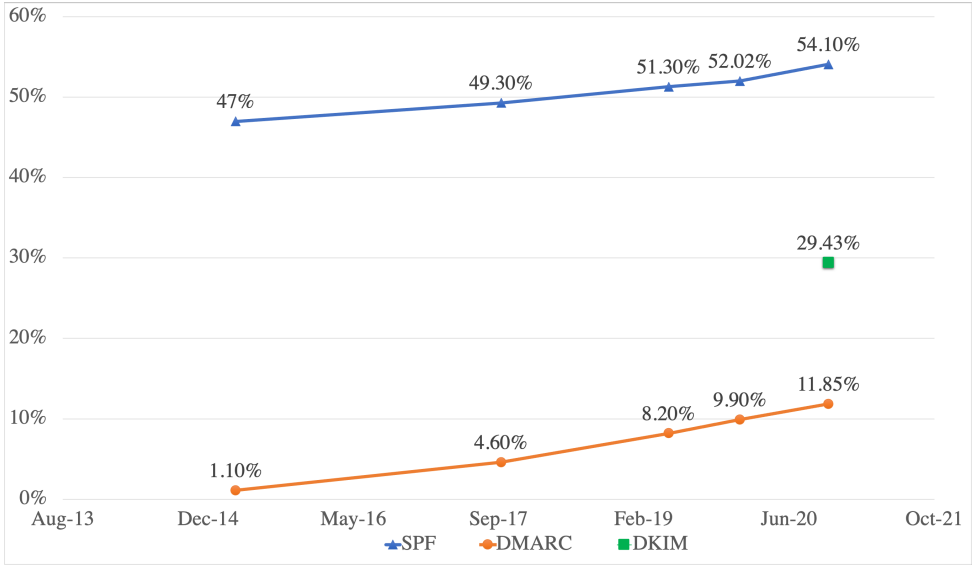
（2）验证通过的身份实体与MIME From身份实体进行对齐

问题似乎都被解决了？

为何钓鱼邮件攻击还是屡禁不止？

邮件安全拓展协议的部署率有限

The result shows that **29.4%** of Alexa Top 1 Million domains have enabled DKIM, of which **2.9%** are misconfigured.



The Adoption Rate of SPF/DKIM/DMARC in Alexa Top 1M Domains

Table 5: DKIM Adoption Rate among Multiple gTLDs.

gTLD	MX Domains	w/ DKIM (%)
.com	371,040	143,156 (38.6%)
.org	33,271	13,787 (41.4%)
.net	33,101	9,926 (30.0%)
.info	5,531	1,443 (26.1%)
.co	3,559	1,453 (40.8%)
.edu	3,062	2,183 (71.3%)
.biz	1,955	534 (27.3%)
.gov	810	431 (53.1%)

Table 6: DKIM Adoption Rate among Multiple ccTLDs.

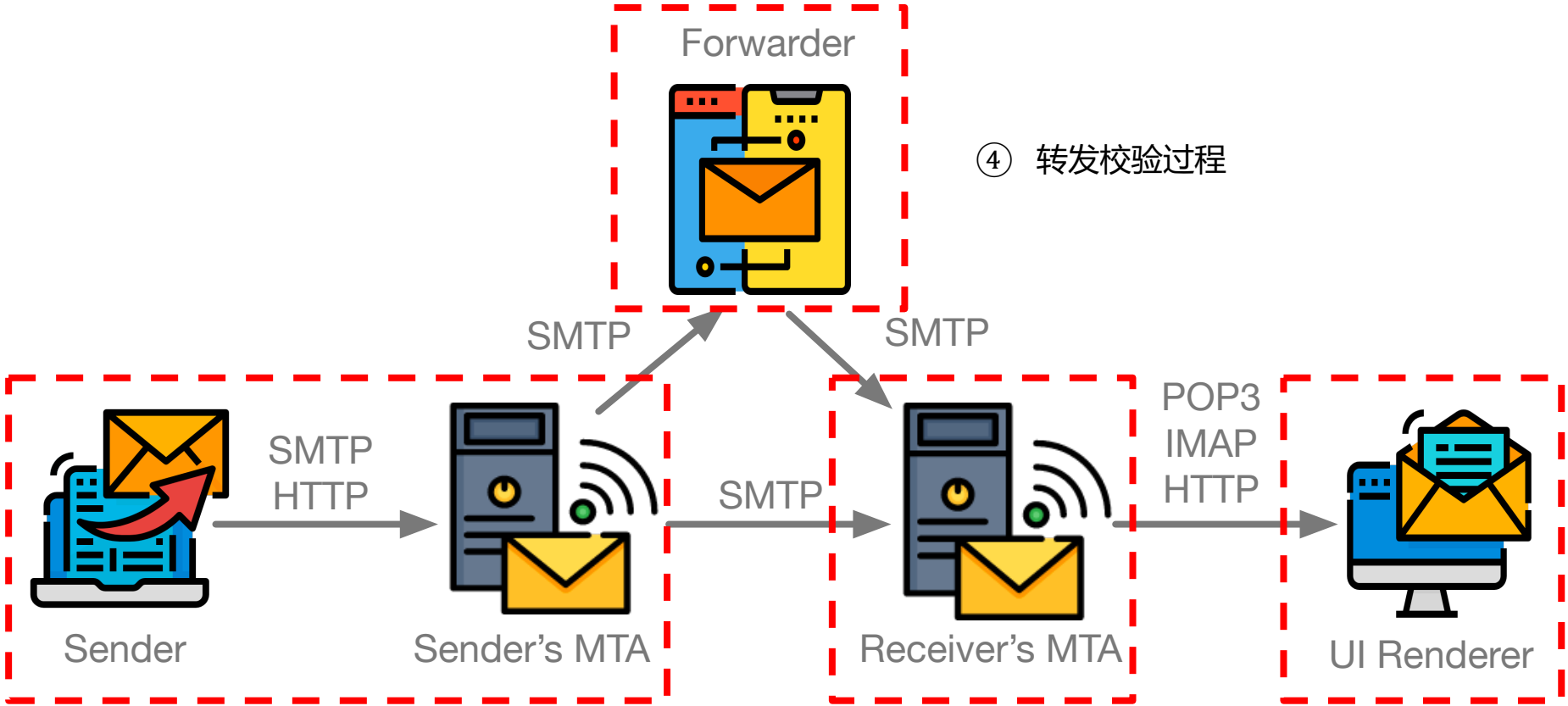
ccTLD	Country	MX Domains	w/ DKIM (%)
.ru	Russia	34,754	12,107 (34.8%)
.de	Germany	25,105	5,744 (22.9%)
.jp	Japan	17,740	2,467 (13.9%)
.uk	United Kingdom	15,496	7,058 (45.6%)
.br	Brazil	13,990	6,737 (48.2%)
.fr	France	11,012	4,141 (37.6%)
.au	Australia	7,452	4,363 (58.6%)
.cn	China	5,439	422 (7.8%)

[1] Security by Any Other Name: On the Effectiveness of Provider Based Email Security (CCS 2015)

[2] End-to-End Measurements of Email Spoofing Attacks (USENIX 2018)

[3] A Large-scale and Longitudinal Measurement Study of DKIM Deployment (USENIX 2022)

让我们重新看一下邮件传输过程

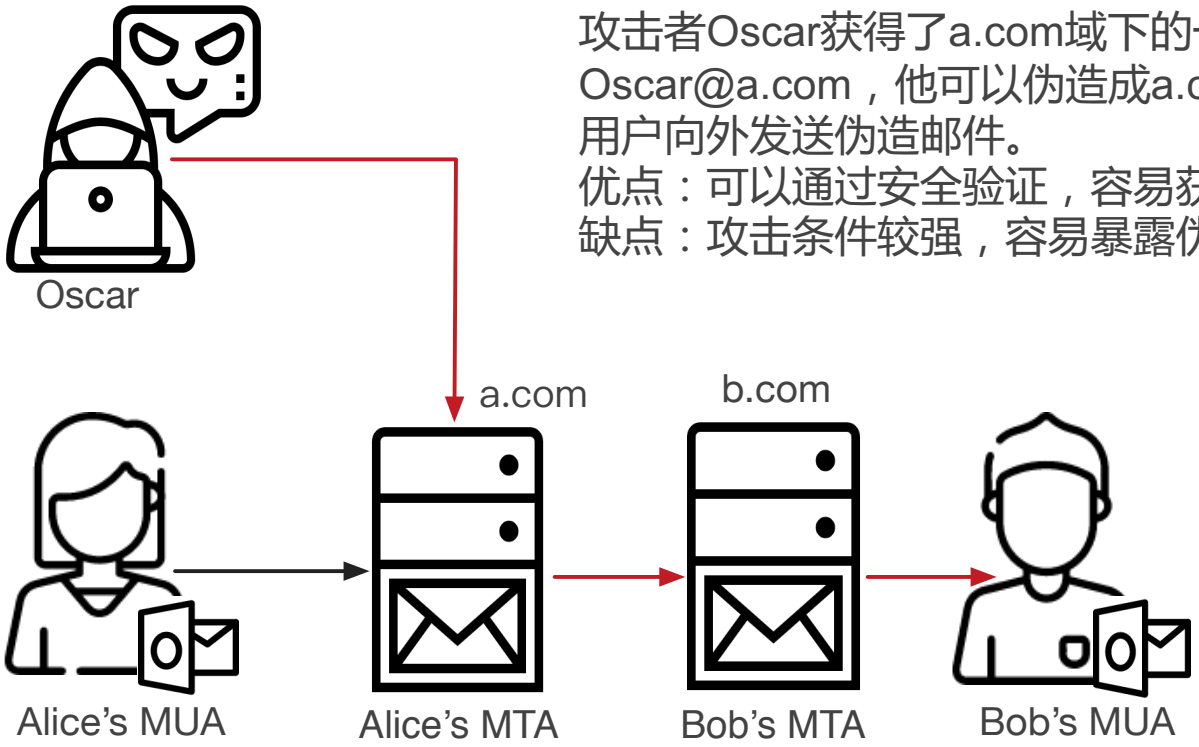


① 发送方身份验证过程　② 接收方身份验证过程　③ 前端显示过程

Attack Models

共享MTA攻击

前提假设：Alice与Bob有邮件往来，Oscar（攻击者）希望伪装成Alice向Bob发信。

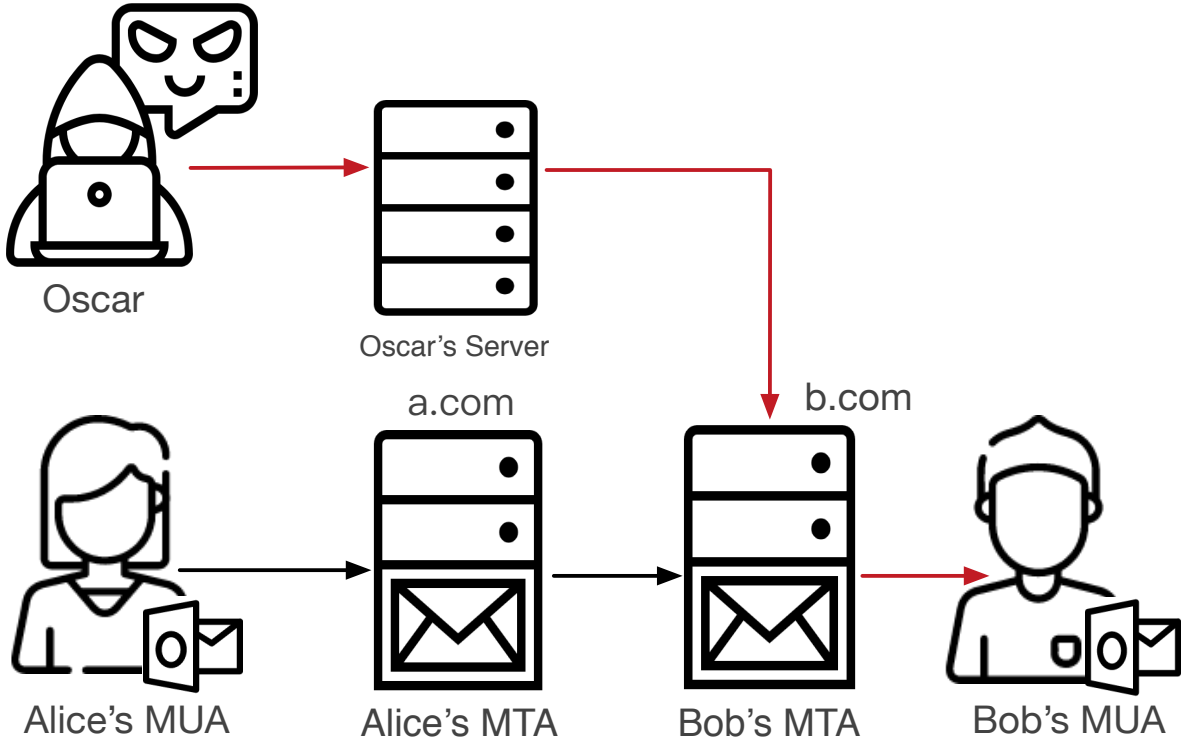


攻击者Oscar获得了a.com域下的一个邮件账号Oscar@a.com，他可以伪造成a.com域下的其他用户向外发送伪造邮件。

优点：可以通过安全验证，容易获得收信人信任

缺点：攻击条件较强，容易暴露伪造痕迹

伪造MTA攻击

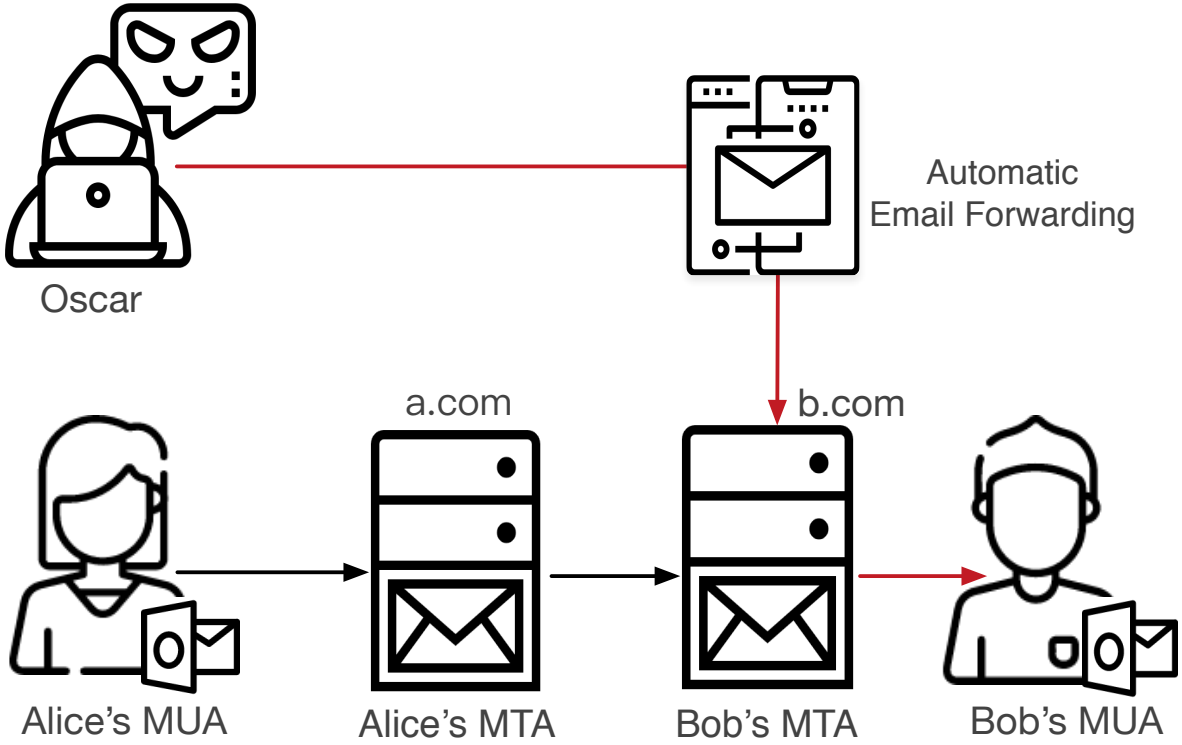


Oscar通过搭建自己的邮件服务器，向外直接发送伪造邮件。

优点：攻击条件相对较弱

缺点：需要绕过接收方防御策略

转发MTA攻击



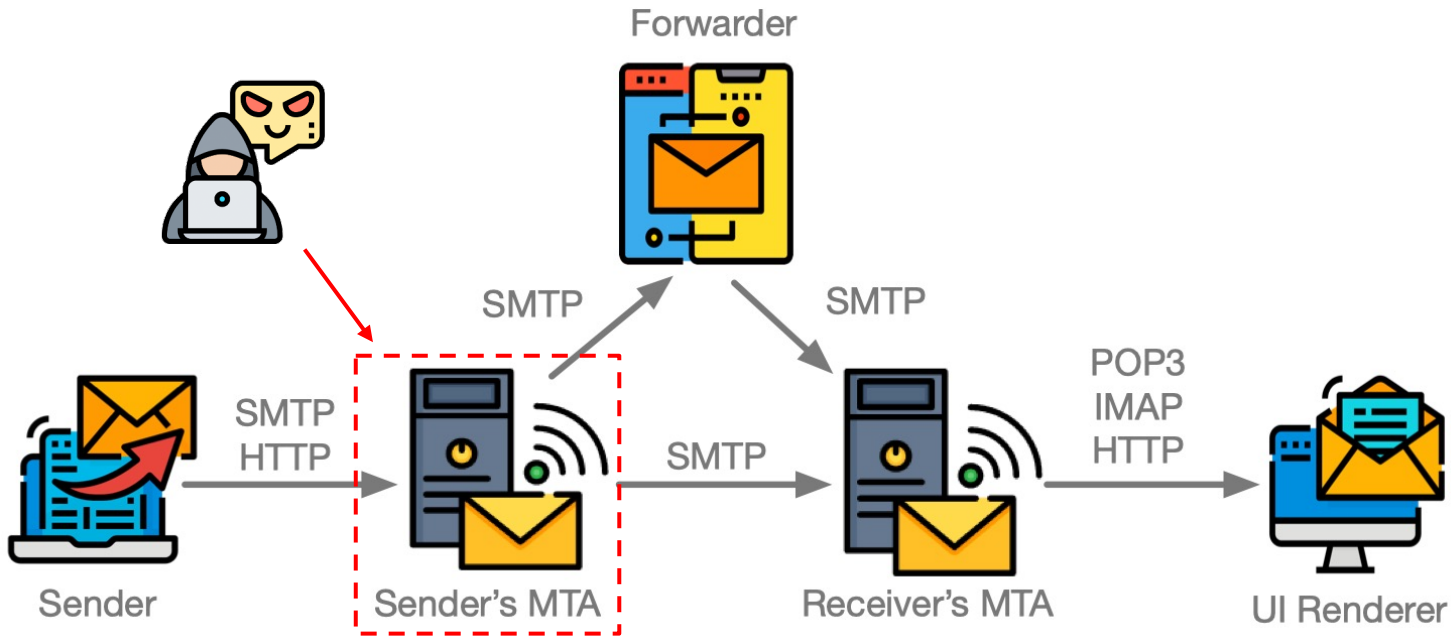
Oscar利用存在问题的邮件转发服务向外发送伪造邮件

优缺点与共享MTA攻击相同

Attack Methods

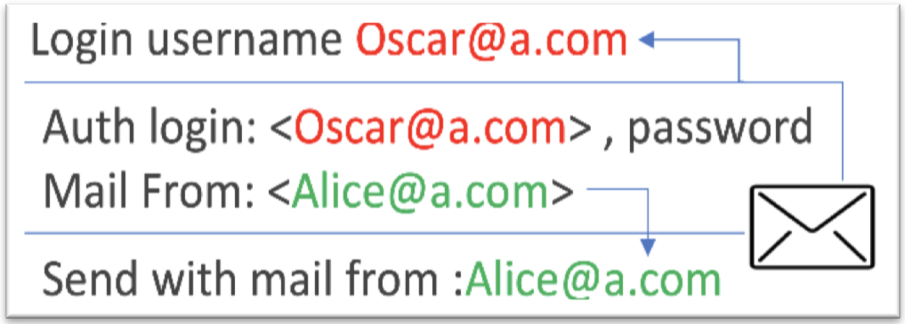
发送方验证阶段的攻击

- **攻击目标:** 让邮件服务发出非账号自身身份的邮件
- **优点：** 可以利用知名邮件服务的IP地址和信誉



发送方验证阶段的攻击

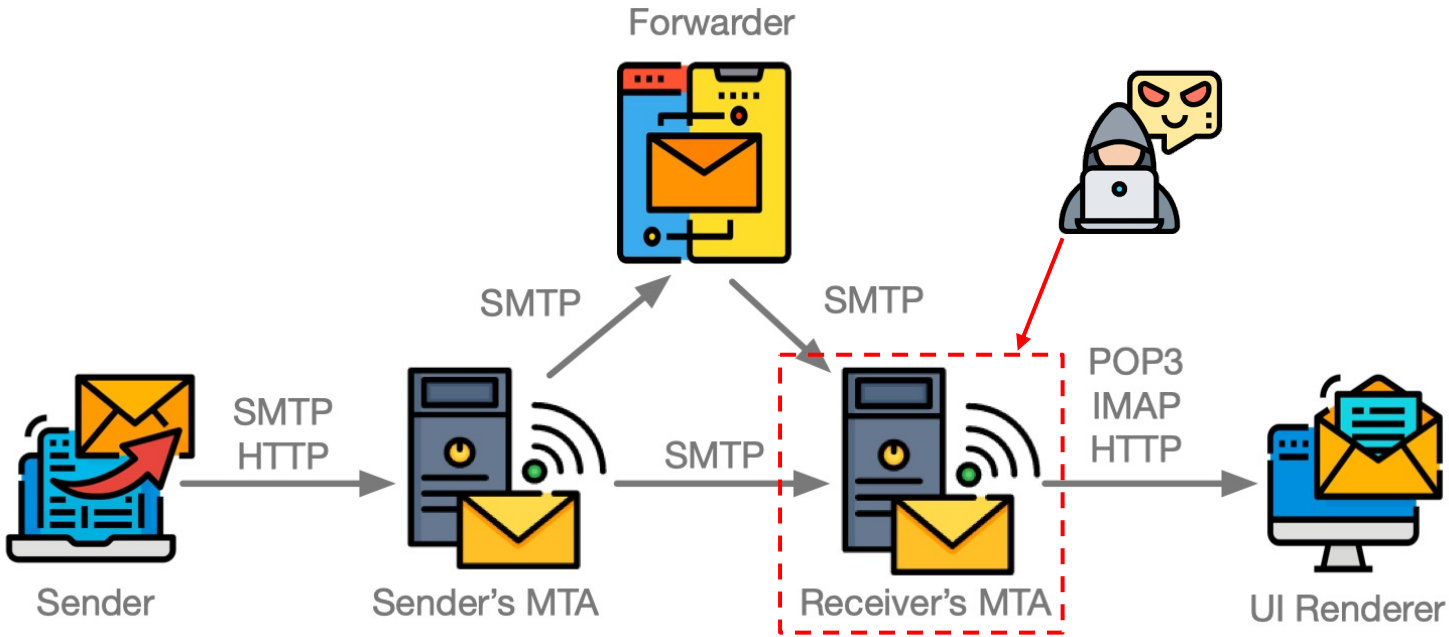
- **Auth Username ≠ Mail From (A1)**



- **Mail From ≠ From (A2)**

针对接收方验证阶段的攻击

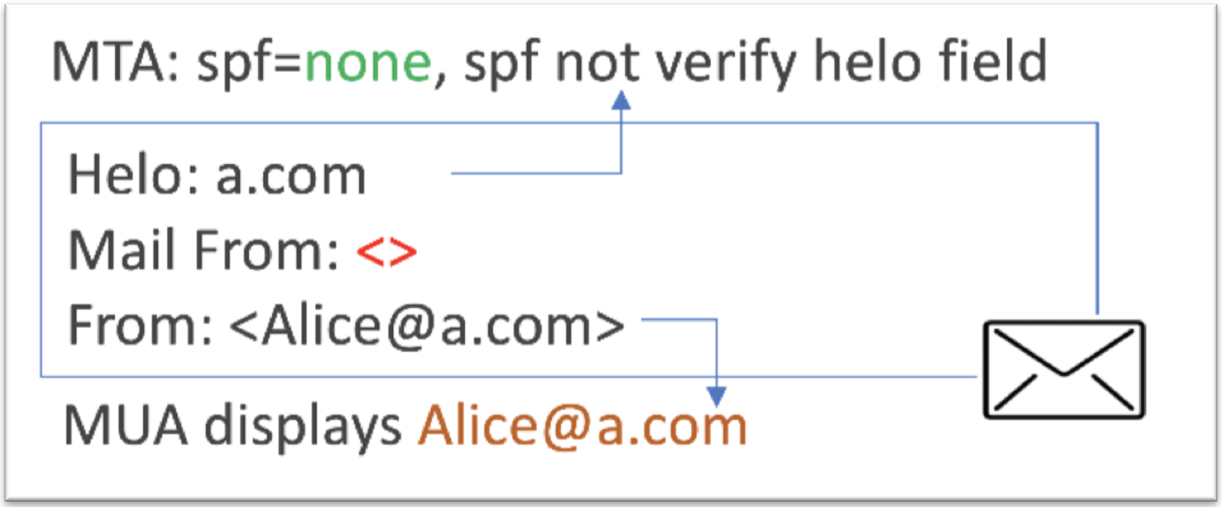
- **攻击目标:** 绕过SPF, DKIM还有DMARC的保护
- **优点:** 顺利通过验证的伪造邮件不太容易被分辨.



针对接收方验证阶段的攻击

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

针对接收方验证阶段的攻击

复杂的From头字段格式

Display Name　Comments　Route portion　Real address

From: Secure (b@b.com) Bank <@c.com, @d.com: a@a.com (e@e.com) > (f@f.com)

不同邮件服务对于异常邮件头字段处理不一致

(a) Parsing inconsistency with route portion.

(b) Parsing inconsistency with "null" mailbox-list.

(c) Parsing inconsistency with comment.

(d) NUL character truncates string parsing.

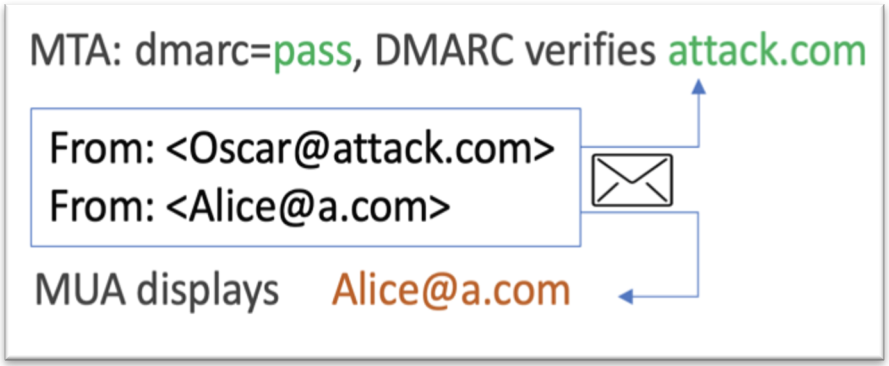
(e) Invisible unicode characters truncate string parsing.

(f) Semantic characters truncate string parsing.

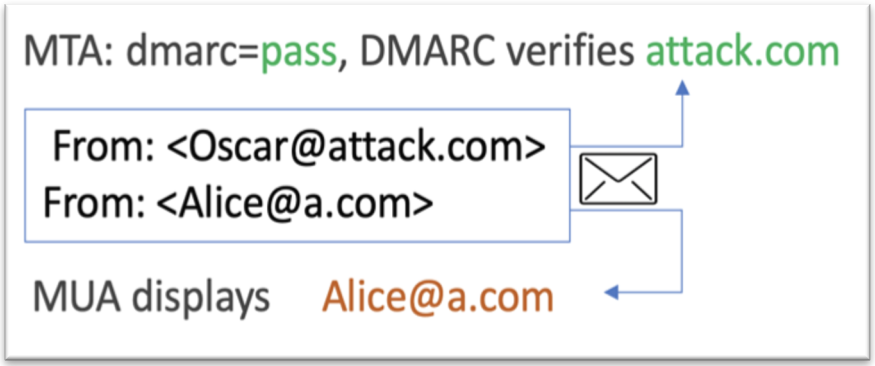
针对接收方验证阶段的攻击

- **Multiple from headers(A4)**

RFC5322规定一封邮件只能有一个From头，但是现实中严格遵守这一规定的邮件服务很少



Ordinary multiple From attack

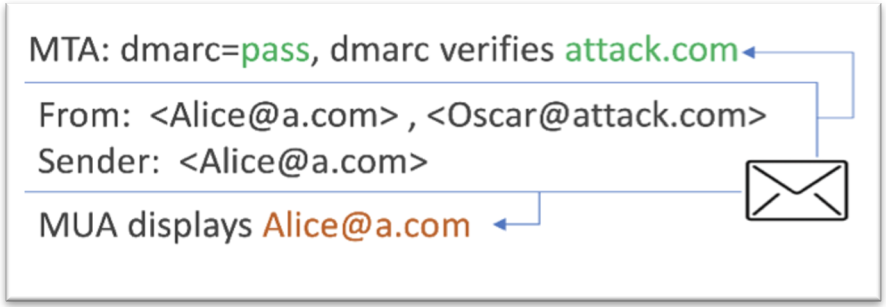


Multiple From attack with spaces

针对接收方验证阶段的攻击

- **Multiple email addresses (A5)**

尽管协议要求一封邮件只能一个From字段，但是一个From字段可以存在多个邮件地址，借助于From字段复杂的格式，我们可以构造一些伪造邮件



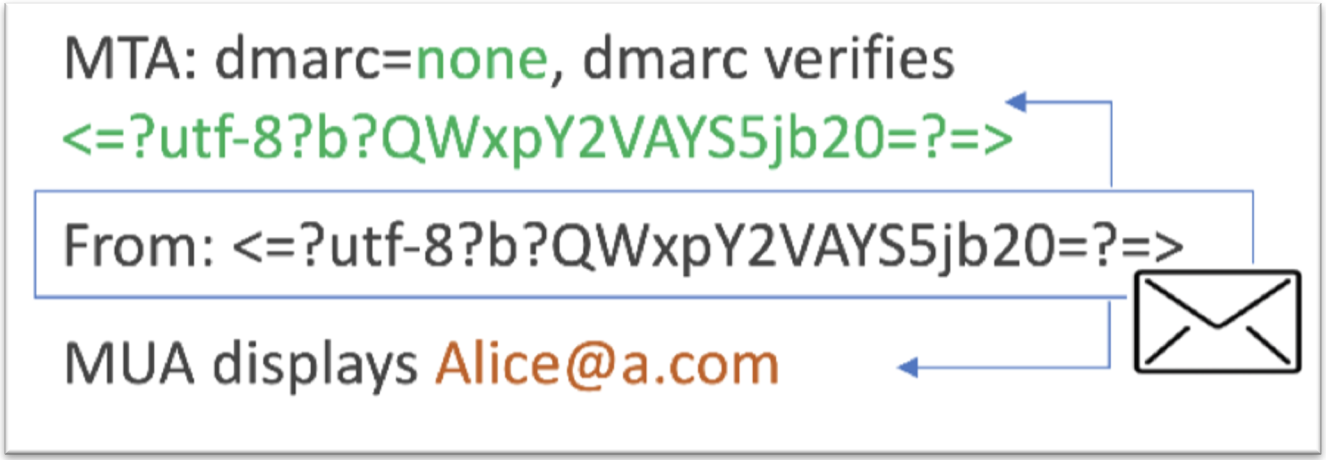
Ordinary multiple address attack

Multiple address attack with comments.

针对接收方验证阶段的攻击

❖ Encoding based attack (A7)

通过对From字段进行特殊的编码（UTF-8）来绕过接收方的DMARC校验

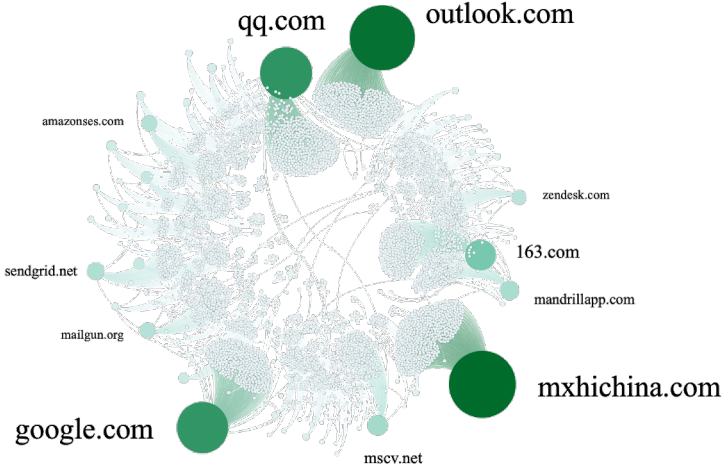


Encoding based attack bypassing DMARC verification

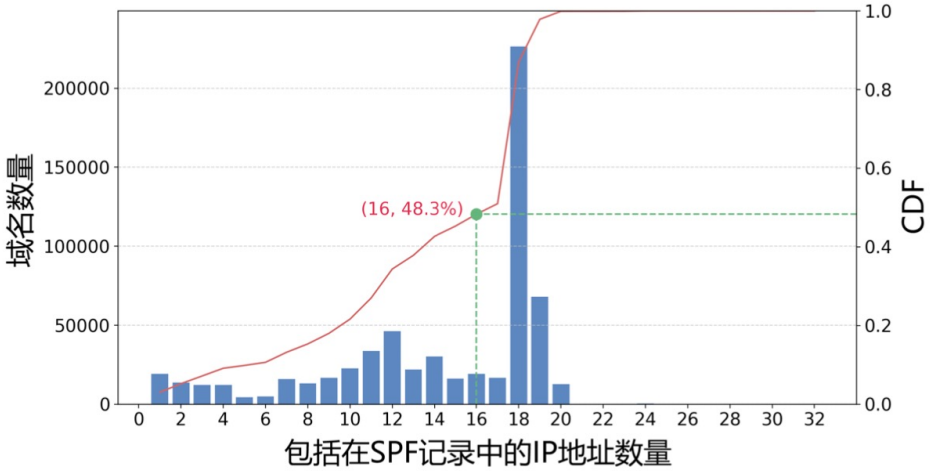
针对接收方验证阶段的攻击（BreakSPF）

➢ SPF的部署现状

- ❖ SPF是目前部署率最高的身份认证协议，部署率达到 **69.8%**。
- ❖ 普遍存在配置宽泛的问题：**51.7%** 的域名在其 SPF 记录中列出了超过 **65,536 (2^{16})** 个 IP 地址
- ❖ 大量域名的SPF记录依赖于邮件提供商的SPF记录。
- ❖ **云服务时代邮件服务集中化破坏SPF基于IP地址的信任模型**



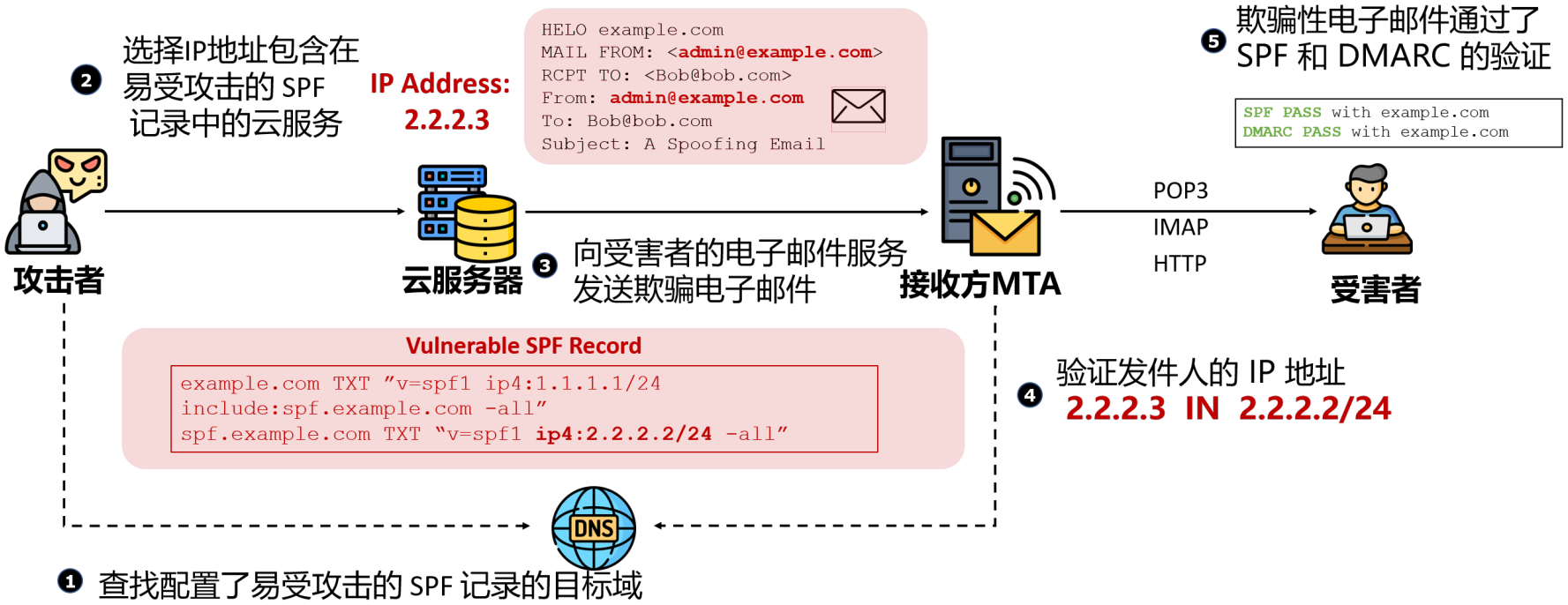
Alexa Top 30,000域名的SPF记录依赖关系图



SPF 记录的 IP 地址覆盖率分析

针对接收方验证阶段的攻击（BreakSPF）

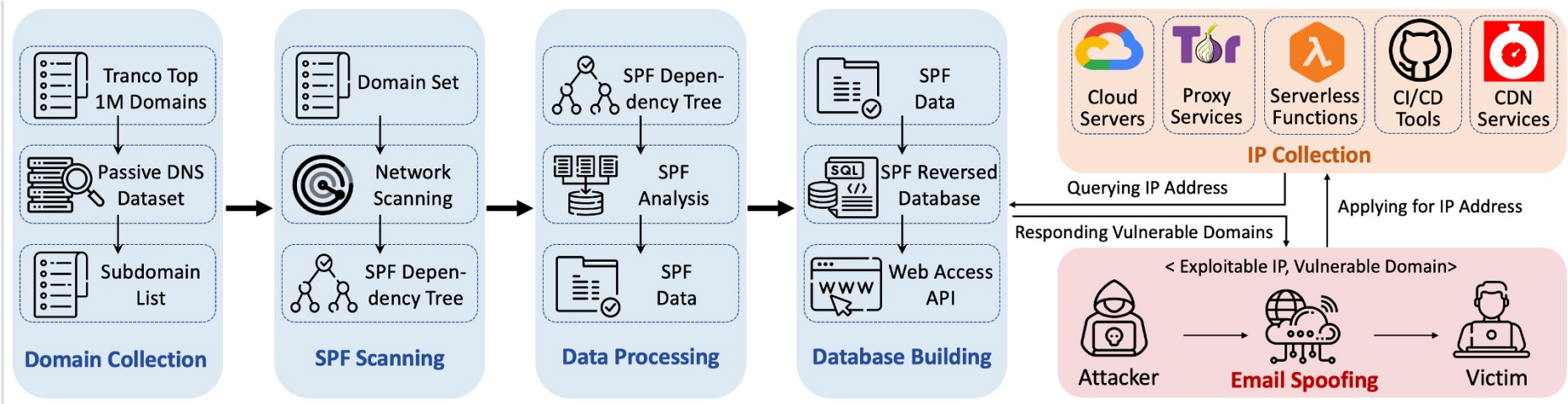
❖ BreakSPF攻击模型



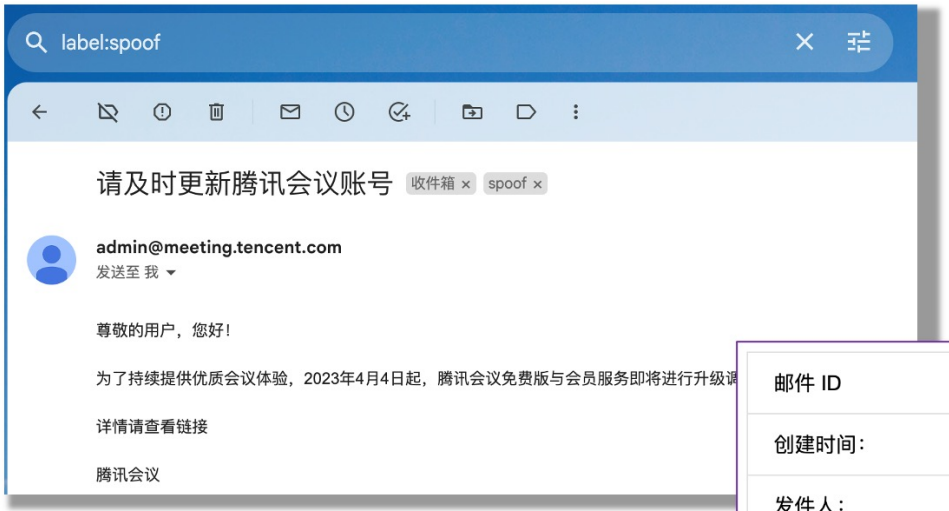
针对接收方验证阶段的攻击（BreakSPF）

提出了一种**新型绕过SPF**的邮件伪造攻击框架，发现了23,916个容易遭受攻击的域名，其中包括**微软、腾讯**等知名域名，再次证明了现有邮件身份认证链的脆弱性。

论文 BreakSPF: How Shared Infrastructures Magnify SPF Vulnerabilities Across the Internet
发表于 NDSS 2024



针对接收方验证阶段的攻击（BreakSPF）



伪造腾讯会议 admin@meeting.tencent.com
向谷歌邮箱（Gmail）发送邮件

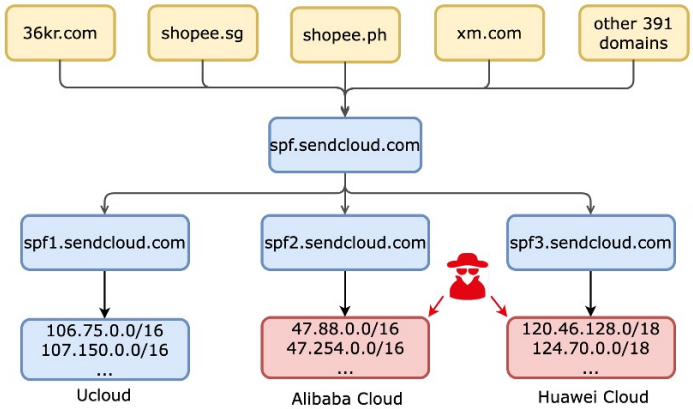
谷歌邮箱的邮件身份认证结果显示伪造邮件，**通过了 SPF 和 DMARC 的校验**

针对接收方验证阶段的攻击（BreakSPF）

利用阿里云服务器成功伪造 **虾皮网 admin@shopee.cn**，并通过SPF验证和DMARC的验证

```
Received: from [172.22.223.181] (unknown [47.88.49.25])
        by localhost.localdomain (Coremail) with SMTP id AQAAfwDnFT0AMVljA34AAA--.5S2;
        Wed, 26 Oct 2022 08:07:13 -0500 (EST)
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Subject: Thank you for shepherding the USENIX paper
From: admin@shopee.cn
To: security@mail1.nospoofing.cn
Date: Wed, 26 Oct 2022 21:07:12 +0800
Return-Path: admin@shopee.cn
X-CM-TRANSID:AQAAfwDnFT0AMVljA34AAA--.5S2
Message-Id:<63593102.000005.32645@coremail.cn>
Authentication-Results: localhost.localdomain; spf=pass smtp.mail=admi
        n@shopee.cn;
```

```
(py36) ➜  Cloud Service dig txt +short shopee.cn | grep spf
"v=spf1 include:spf.sendcloud.org include:spf.mail.qq.com include:_spf.salesforc
e.com include:mailgun.org ~all"
(py36) ➜  Cloud Service dig txt +short spf.sendcloud.org | grep spf
"v=spf1 include:spf1.sendcloud.org include:spf2.sendcloud.org include:spf3.sendc
loud.org -all"
(py36) ➜  Cloud Service dig txt +short spf2.sendcloud.org | grep spf
"v=spf1 ip4:161.117.0.0/16 ip4:47.241.0.0/16 ip4:47.251.0.0/16 ip4:47.254.0.0/16
 ip4:47.74.0.0/16 ip4:47.88.0.0/16 ip4:47.89.0.0/16 ip4:47.91.0.0/16 ip4:8.214.0
.0/16 -all"
```



针对接收方验证阶段的攻击（Bypass DKIM）

- DKIM的重放攻击
  利用DKIM的特性，替换DKIM未保护的字段

```
DKIM-Signature: v=1; l=1850; d=example.com; s=20140901;
h=date:from:to:message-id:subject:mime-version; b=...; bh=...
From: Support <support@example.com>
To: original-receiver
Subject: A Normal Email
Content-Type: multipart/mixed; boundary=-----=_Part_9797977
------=_Part_9797977
Content-type: text/plain

Email Content...
------=_Part_9797977
```

针对接收方验证阶段的攻击（Bypass DKIM）

- DKIM的重放攻击
  利用DKIM的特性，替换DKIM未保护的字段

```
DKIM-Signature: v=1; l=1850; d=example.com; s=20140901;
h=date:from:to:message-id:subject:mime-version; b=...; bh=...
From: Support <support@example.com>
To: victim@victim.com
To: original-receiver
Subject: A Spoofing Email
Subject: A Normal Email
Content-Type: multipart/mixed; boundary=----=_Part_9797977
------=_Part_9797977
Content-type: text/plain

Email Content...
------=_Part_9797977
```

针对接收方验证阶段的攻击（Bypass DKIM）

- DKIM的重放攻击
  如果DKIM签名使用了l标签，但是有没有对Content-Type字段签名，会造成更糕的情况

```
DKIM-Signature: v=1; l=1850; d=example.com; s=20140901;
h=date:from:to:message-id:subject:mime-version; b=...; bh=...
From: Support <support@example.com>
To: victim@victim.com
To: original-receiver
Subject: A Normal Email
Content-Type: multipart/mixed; boundary=BAD
Content-Type: multipart/mixed; boundary=------_Part_9797977
------_Part_9797977
Content-type: text/plain
Email Content...
------_Part_9797977
--BAD
Content-type: text/plain
This is a faked mail with valid DKIM signature from example.com.
--BAD--
```

针对接收方验证阶段的攻击（Bypass DKIM）

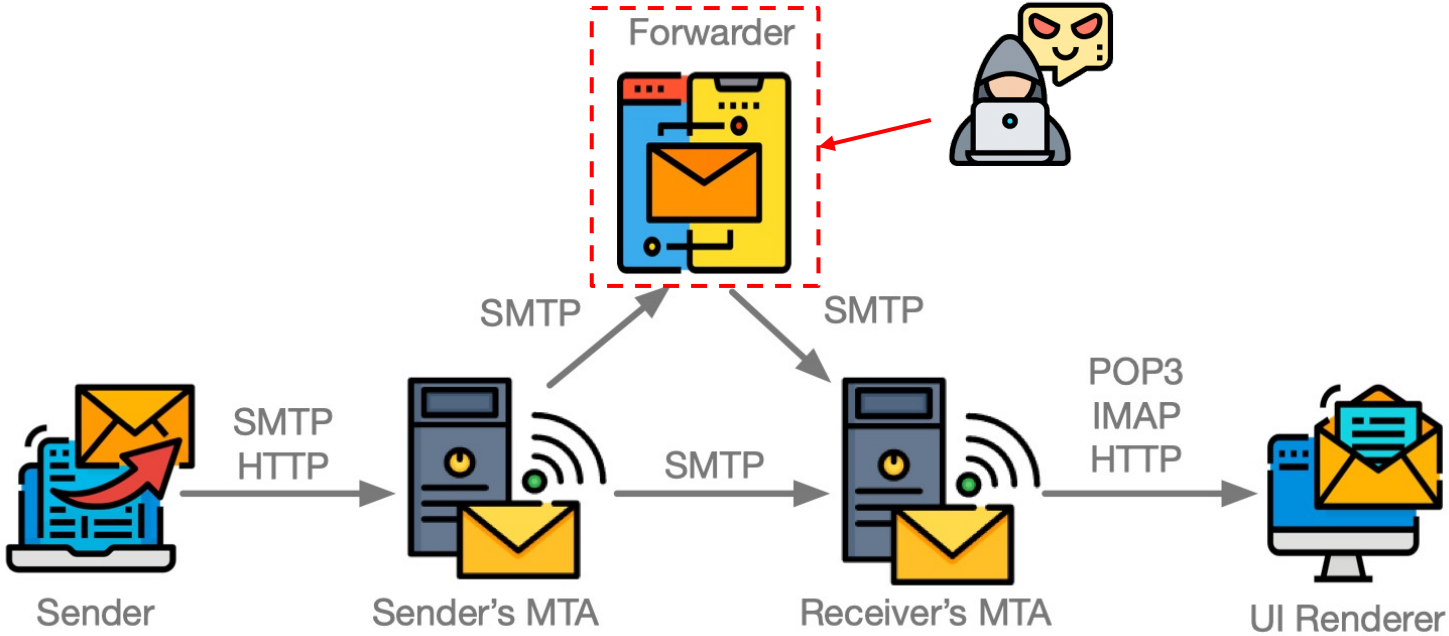
❖ 利用\00截断

```
DKIM-Signature: v=1; l=1850; d=example.com;
s=attacker.com\x002019;
h=date:from:to:message-id:subject:mime-version; b=...; bh=...
From: Support <support@example.com>
To: original-receiver
Subject: A Spoofing Email
Content-Type: multipart/mixed; boundary=BAD
--BAD
Content-type: text/plain

This is a faked mail with valid DKIM signature from example.com.

--BAD--
```

针对邮件转发验证阶段的攻击

攻击目标:

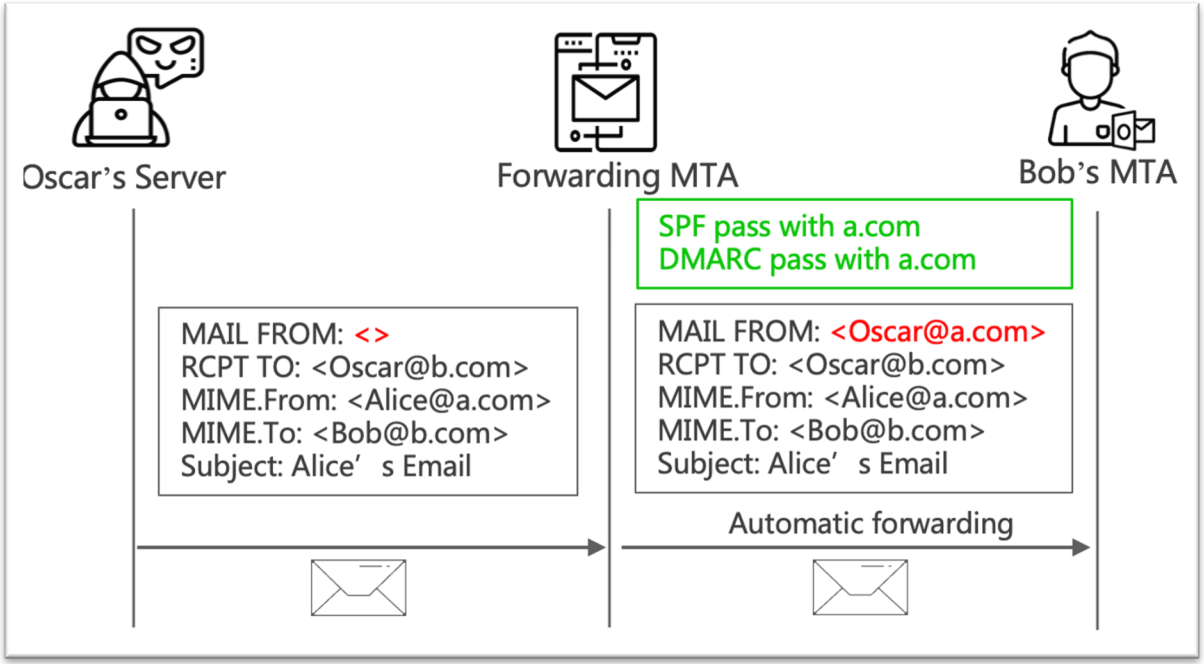
- 可以自由配置转发服务且不需要验证的邮箱
- 获得更高的安全担保，更易进入用户的收件箱



针对邮件转发验证阶段的攻击

Unauthorized Forwarding Attack (A9)

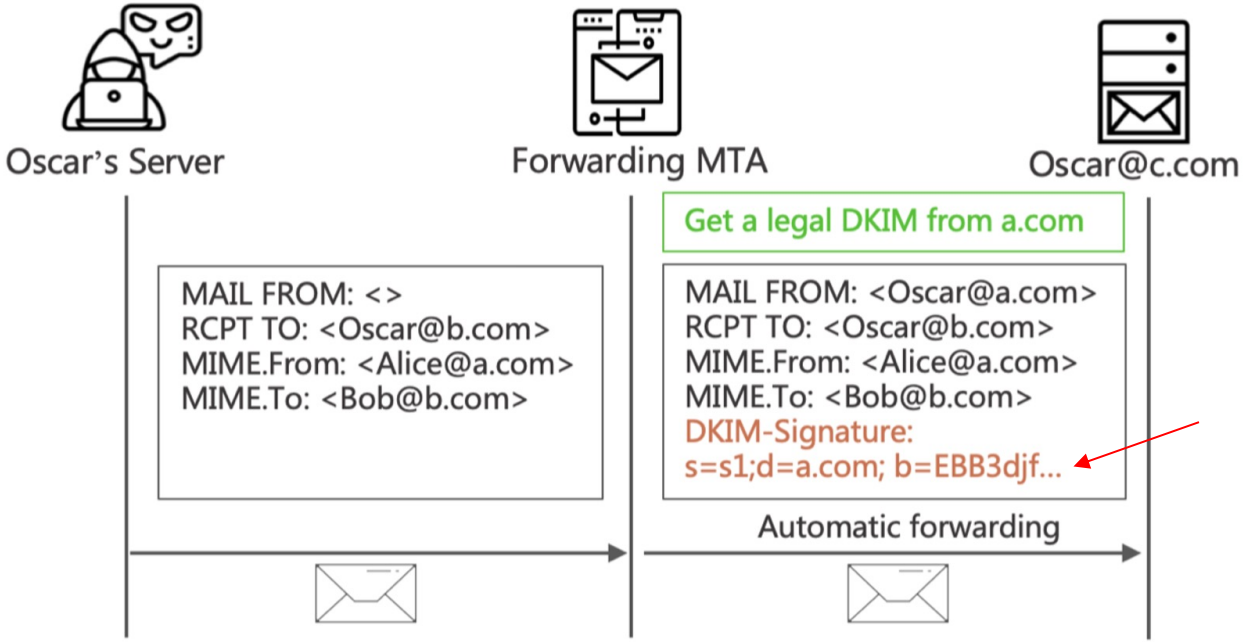
- 如果邮件转发服务不需要验证，我们可以利用邮件转发服务帮我们绕过SPF和DMARC的验证



针对邮件转发验证阶段的攻击

DKIM-Signature Fraud Attack (A10)

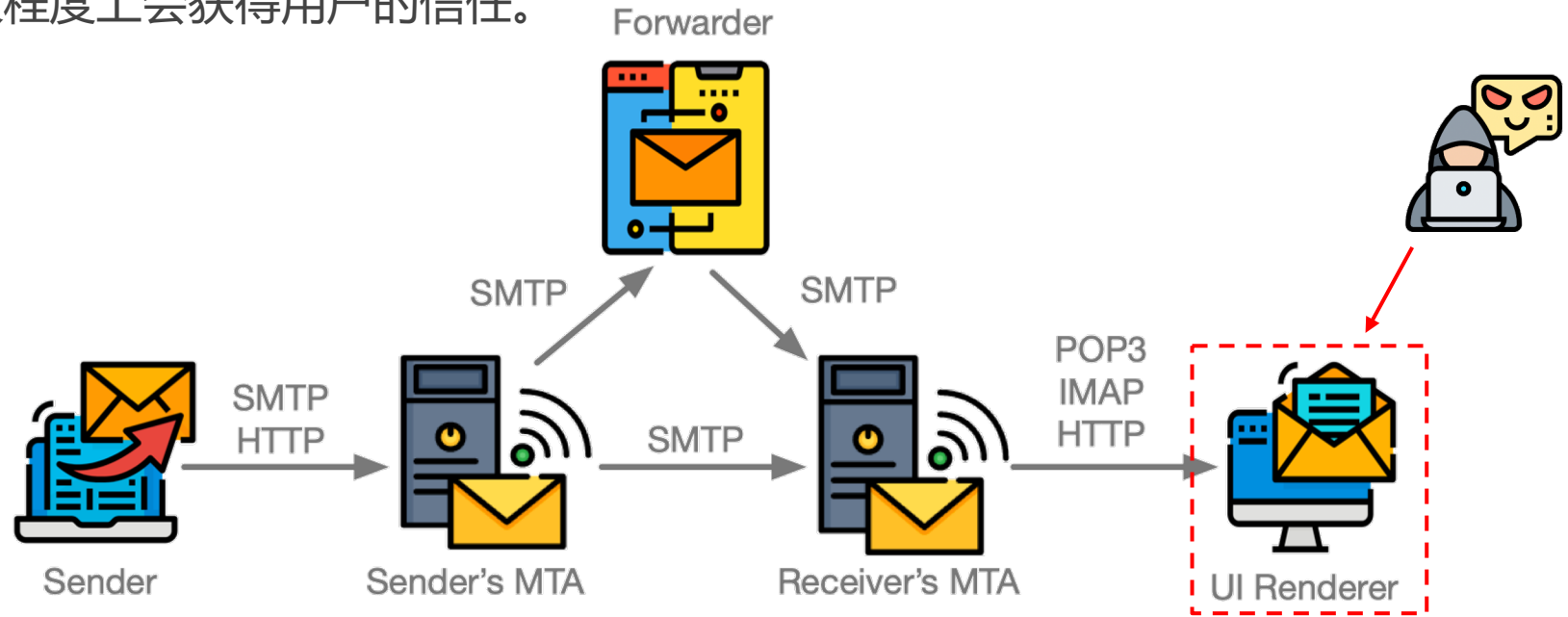
- 如果邮件转发服务不加验证的添加自己的DKIM签名，我们可以通过这种方式拿到合法的DKIM签名



针对前端显示阶段的攻击

攻击目标:

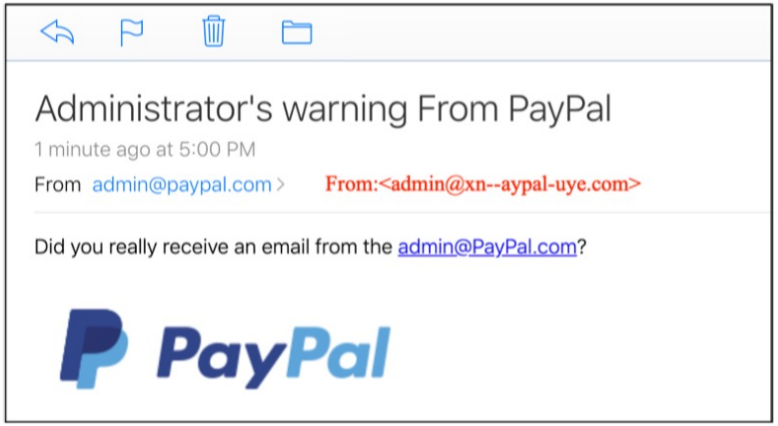
- 让前端显示的邮件发信人与真实的发信人不符。
- 前端显示是用户看到邮件前的最后一环，如果界面上没有触发任何的安全提醒，极大程度上会获得用户的信任。



针对前端显示阶段的攻击

复杂灵活的邮件显示

- Internationalized domain names + email address internationalization (**EAI**)
- 国际化域名(**IDN**) 的显示让邮件地址中可以出现Unicode编码的字符，这引入了一些新的攻击场景。



IDN homograph attack (A12)

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

Missing UI Rendering Attack (A13)

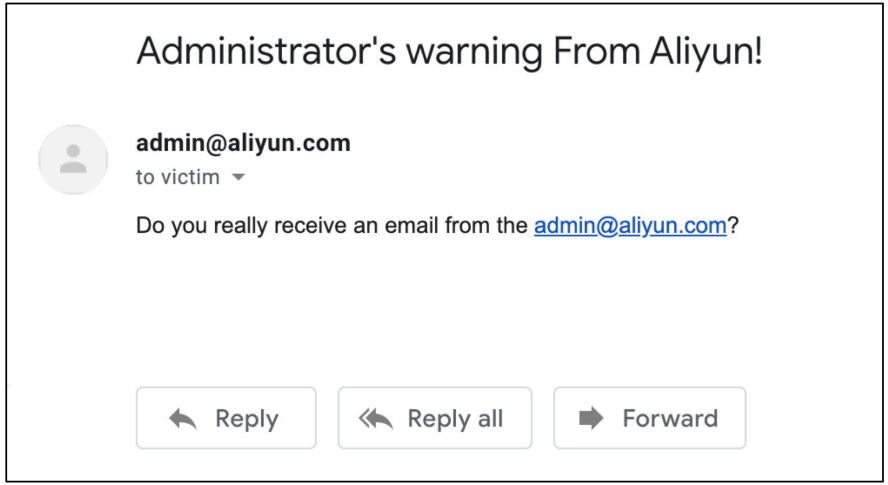
\u202emoc.a@\u202dalice ==> Alice@a.com

Right-to-left Override Attack (A14)

Case Study

攻击案例 1

现实世界中大多数邮件提供商已经部署了一定的防御措施，单一的攻击方法没有办法绕过所有的防御策略，成功率并不高。所以我们在实际测试中往往讲多种攻击方法组合使用，这样可以让伪造效果更加逼真，也有利于绕过现有防御策略。



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

admin@aliyun.com → victim@gmail.com

攻击案例 1

Oscar's Server

Direct MTA Attack with A2,A3

Aliyun's MTA

Forward MTA Attack with A11

Oscar's MTA

MAIL FROM: <>
RCPT TO: <Oscar@aliyun.com>

From: <admin@aliyun.com>
To: <victim@gmail.com>
Subject:Administrator's warning From Aliyun

MAIL FROM: <Oscar@aliyun.com>
RCPT TO: <Oscar@attack.com>

From: <admin@aliyun.com>
To: <victim@gmail.com>
Subject: Administrator's warning From Aliyun
DKIM-Signature: v=1; d=aliyun.com;
h=Content-Type:Subject:From:To; bh=IOC…

攻击案例 1

Oscar's Server

Direct MTA Attack
with Legal DKIM signature

Gmail's MTA

Verify and render email

Victim's MUA

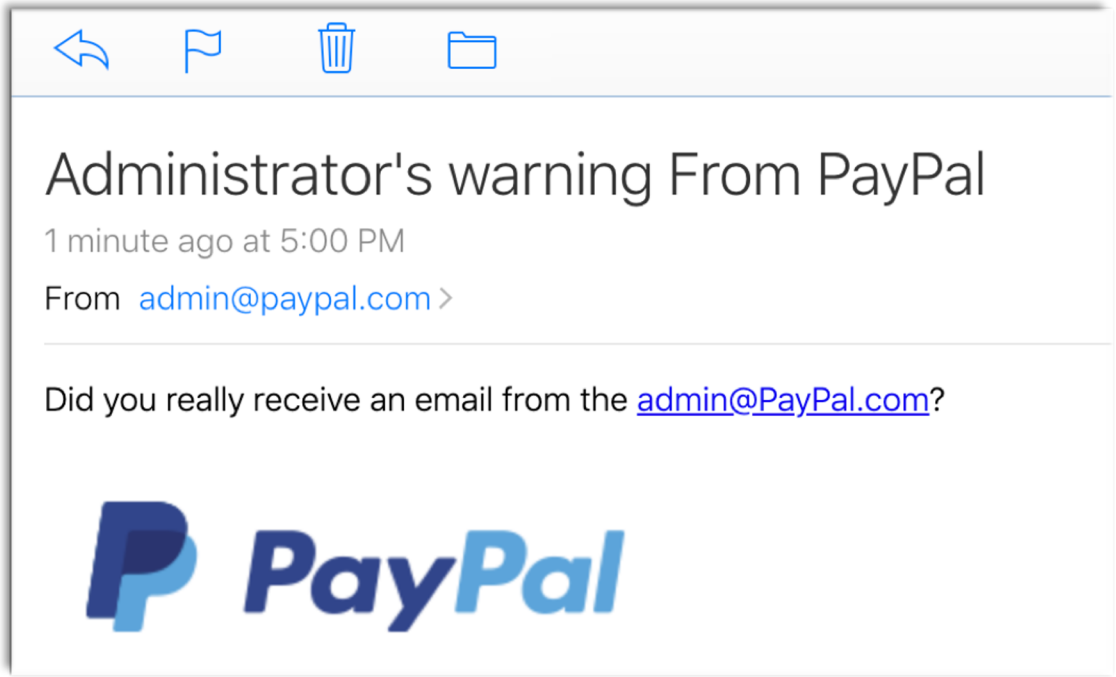
MAIL FROM: <admin@attack.com>
RCPT TO: <victim@gmail.com>

From: <admin@aliyun.com>
To: <victim@gmail.com>
Subject: Administrator's warning From Aliyun
DKIM-Signature: v=1; d=aliyun.com;
h=Content-Type:Subject:From:To; bh=IOC...

MTA:
SPF verifies attack.com, spf=pass,
DKIM verifies aliyun.com, dkim=pass,
DMARC verifies aliyun.com, dmarc=pass.
Oscar can control the SPF record of attack.com

MUA displays admin@aliyun.com and no any security indicators on UI

攻击案例 2



admin@paypal.com → victim@icloud.com

攻击案例 2

- DKIM签名是yahoo签发的，可以通过验证
- DMARC与第一个From对齐
- 前端显示第二个From
- 这里体现了不同环节验证身份信息的不一致性

Oscar's MUA

Login MTA Attack with A2, A3

Yahoo's MTA

Verify and render email

iCloud's MTA

MAIL FROM: <Oscar@yahoo.com>
RCPT TO: <victim@icloud.com>

From: <Oscar@yahoo.com>
From: <Admin@paypal.com>
To: <victim@gmail.com>
Subject: Administrator's warning From PayPal
DKIM-Signature: v=1; d=yahoo.com; h=Content-Type:Subject:From:To; bh=IOC...

MAIL FROM: <Oscar@yahoo.com>
RCPT TO: <victim@icloud.com>

From: <Oscar@yahoo.com>
From: <Admin@paypal.com>
To: <victim@gmail.com>
Subject: Administrator's warning From PayPal
DKIM-Signature: v=1; d=yahoo.com; h=Content-Type:Subject:From:To; bh=IOC...

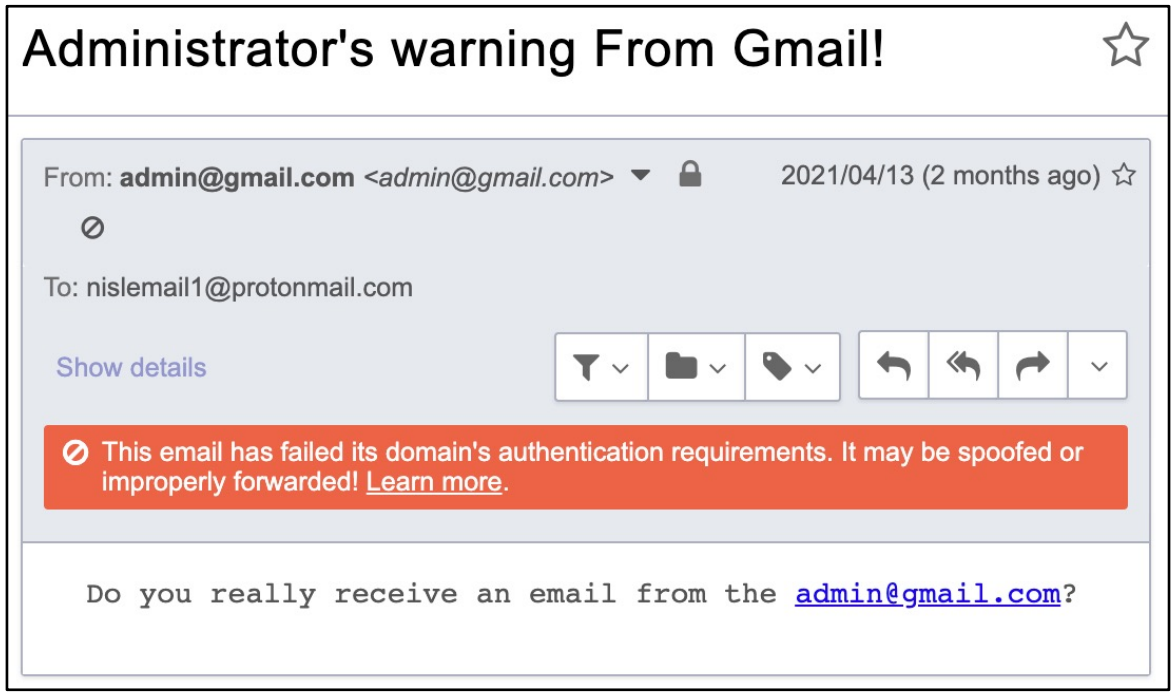
Note: Yahoo Mail forbid users from sending email with different Mail From and From headers.
But we can bypass it through multiple From attack(A3)

iCloud's MTA: The spoofing email passed all email protocol verification with yahoo.com, but the MUA's UI shows the sender: Admin@paypal.com

攻击案例 3

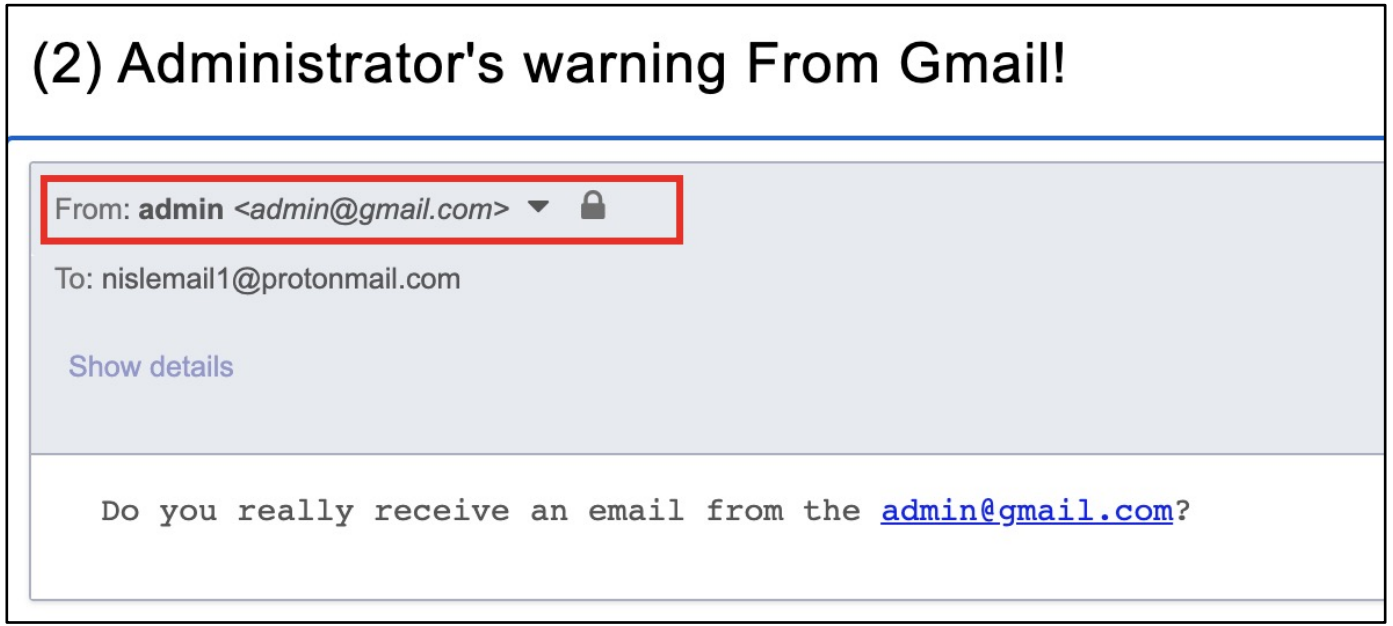
简单的测试后发现我们可以伪造admin@sina.com（未配置DMARC服务的域名）发送伪造邮件，且界面上没有任何UI提醒

攻击案例 3



尝试伪造成Gmail向Protonmail邮箱发信，发现发信被拦截到了垃圾箱中，同时触发了Protonmail的安全提醒，那如果我们想伪造配置了DMARC服务的域名要怎么办呢？

攻击案例 3



MAIL From: attacker@anydomain.com

MIME From: admin<\u202emoc.liamg@nimda\u202c>

Conclusion

攻击的现实影响

- 我们对30家流行的邮件服务提供商还有23个常用的邮件客户端进行了测试。

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}

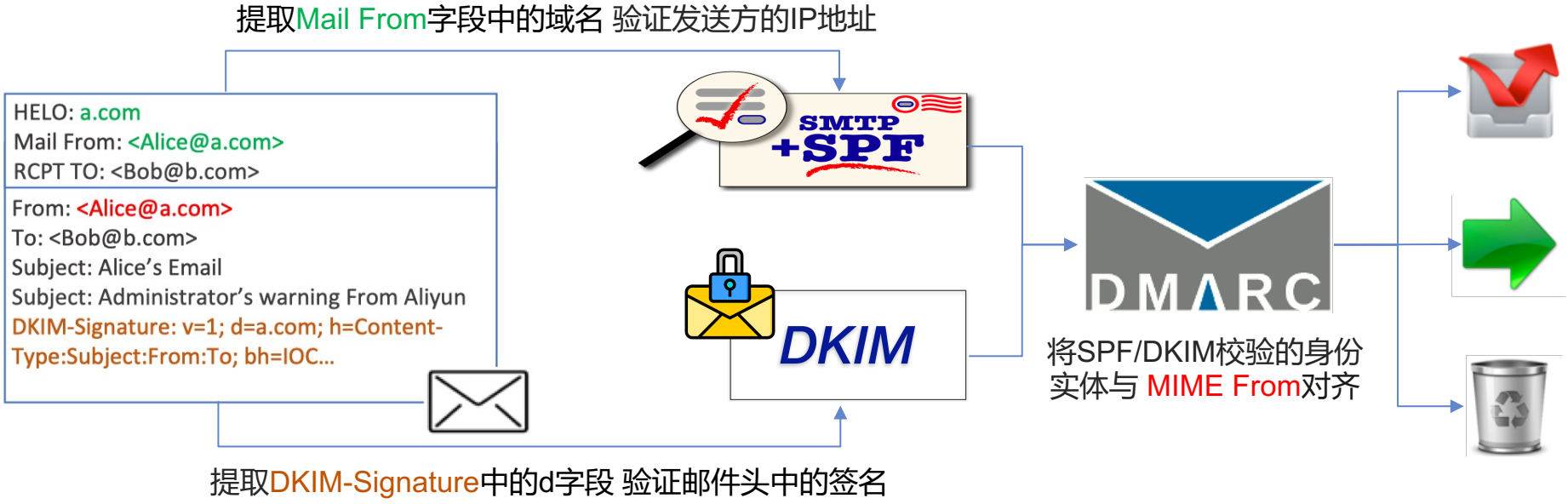
OS	Clients	SIC	Weaknesses
Windows	Foxmail	✓	A_6, A_7, A_{13}, A_{14}
	Outlook	✓	A_6, A_{13}
	eM Client	✓	A_6, A_{12}
	Thunderbird		A_6, A_{13}, A_{14}
	Windows Mail		A_6, A_7, A_{13}, A_{14}
MacOS	Foxmail		A_6, A_{13}
	Outlook	✓	A_6, A_{13}
	eM Client	✓	A_6, A_7, A_{12}, A_{13}, A_{14}
	Thunderbird		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}

邮件伪造攻击频发的内在原因是什么？

木桶理论：Weak Links in Authentication Chains

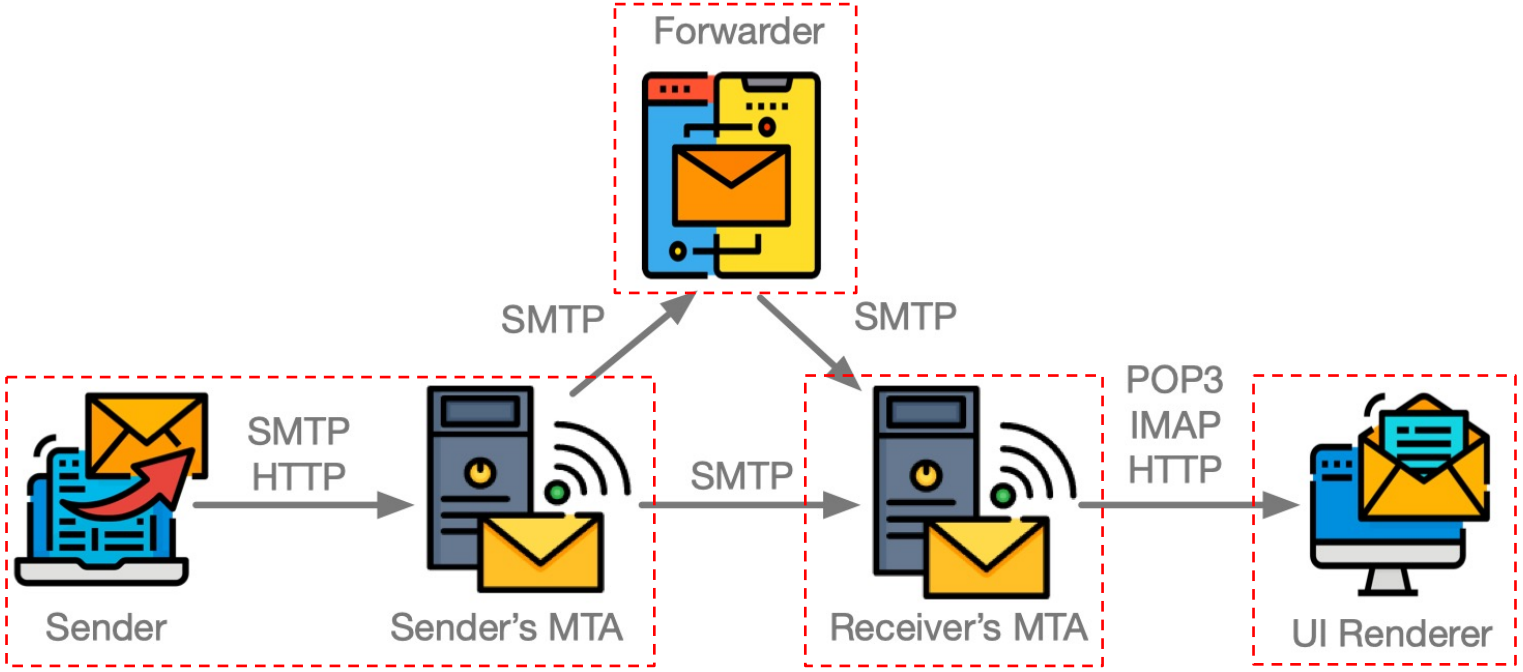
Weak Links among Multi-protocols

由于邮件身份验证的过程需要不同的协议相互配合，但不同的安全拓展协议保护的身份实体不一致，因此攻击能够达成。



Weak Links among Multi-roles

邮件传输过程中的四个不同环节（发送方、接收方、转发方和前端显示）需要承担不同的安全义务，一个环节出现问题就会给攻击者可乘之机。



Weak Links among Multi-services

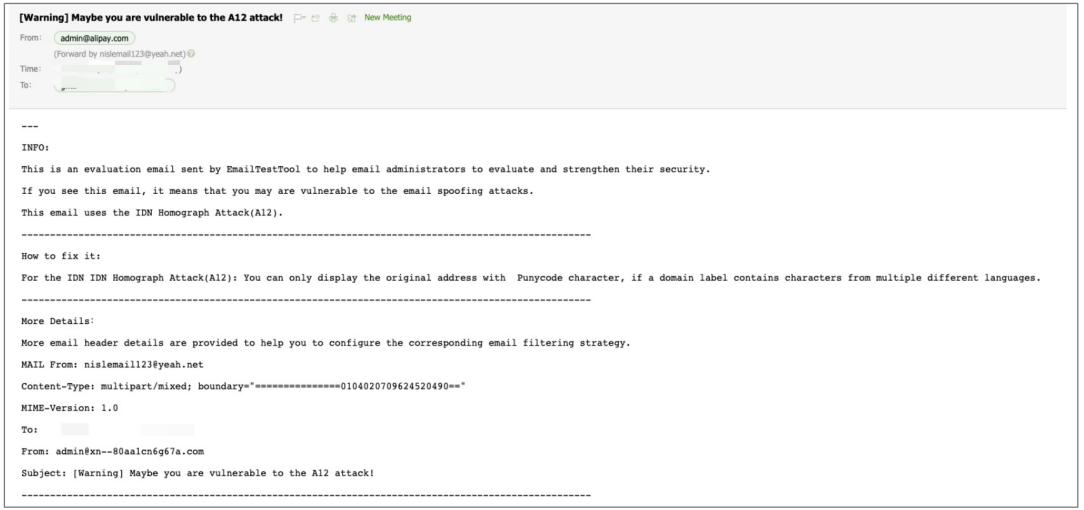
- 不同的邮件服务有不同的安全配置和实现方式，这种不一致会导致对歧义邮件理解的不一致
- 很多邮件服务的实现其实与RFC协议的规定并不一致

这些不一致都可能存在安全风险

QQ邮箱 mail.qq.com
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

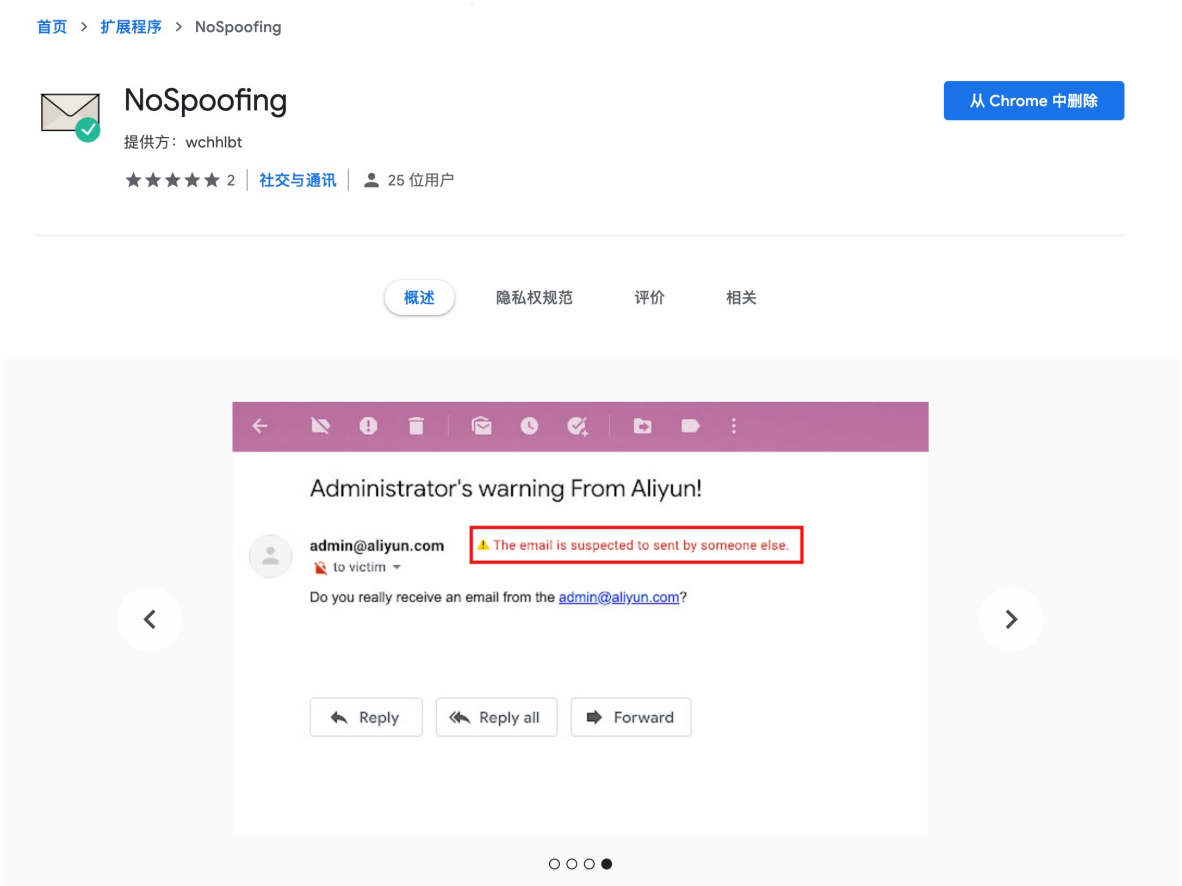
检测工具 ESpoofing



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

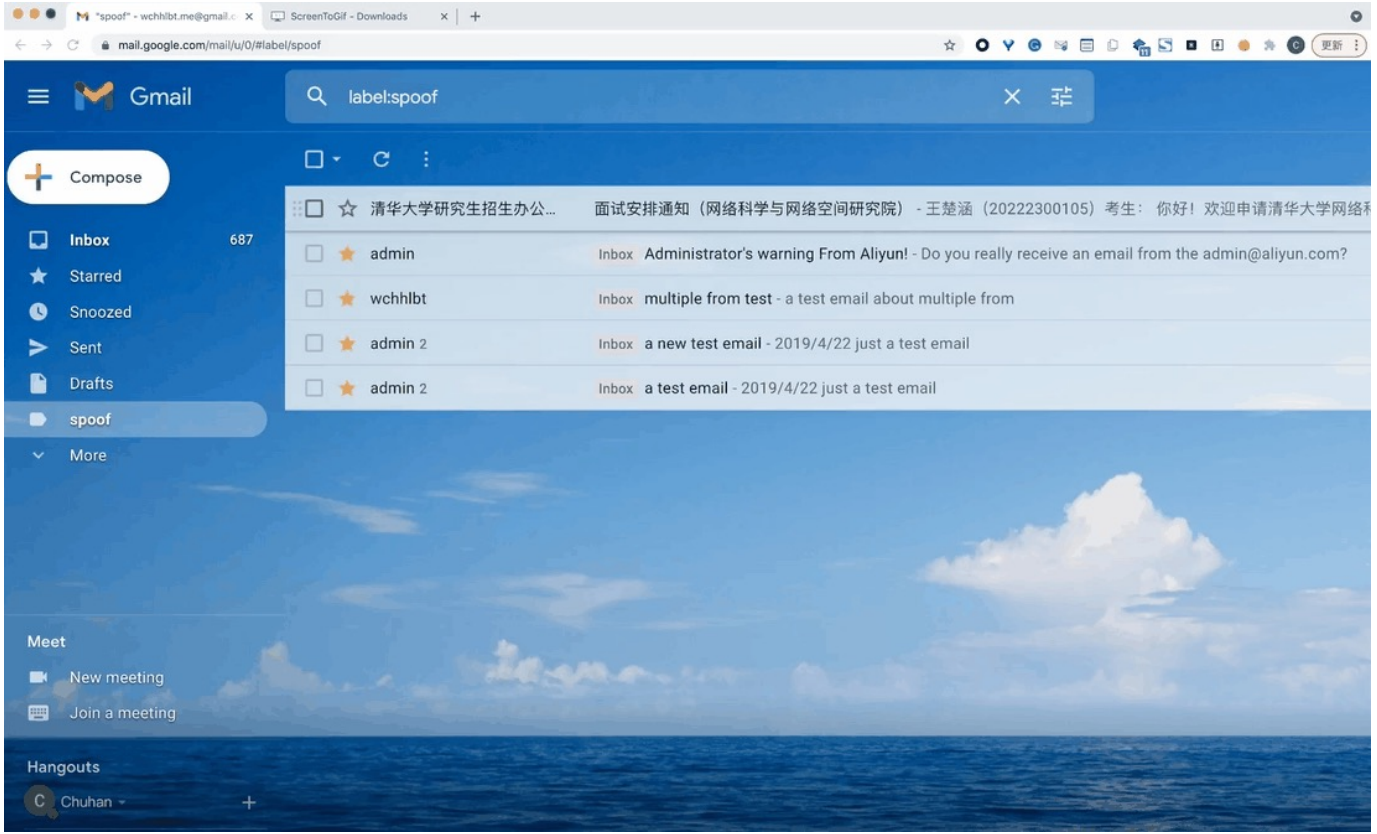
https://github.com/wchhlbt/Email-Spoofing-Test-Tools

Chrome 插件 NoSpoofing



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

Chrome 插件 NoSpoofing



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

邮件安全的相关工作

邮件伪造攻击

1. 【USENIX 2020】Composition Kills: A Case Study of Email Sender Authentication
2. 【USENIX 2021】Weak Links in Authentication Chains: A Large-scale Analysis of Email Sender Spoofing Attacks
3. 【USENIX 2018】End-to-End Measurements of Email Spoofing Attacks

S/MIME & PGP 安全

1. 【USENIX 2018】Efail: Breaking S/MIME and OpenPGP Email Encryption using Exfiltration Channels
2. 【USENIX 2019】"Johnny, you are fired!" - Spoofing OpenPGP and S/MIME Signatures in Emails
3. 【CCS 2020】Mitigation of Attacks on Email End-to-End Encryption

邮件协议测量

1. 【 CCS 2015】Security by Any Other Name: On the Effectiveness of Provider Based Email Security
2. 【IMC 2015】Neither Snow Nor Rain Nor MITM . . . An Empirical Analysis of Email Delivery Security
3. 【USENIX 2022】A Large-scale and Longitudinal Measurement Study of DKIM Deployment

其他

1. 【 S&P 2019】Characterizing Pixel Tracking through the Lens of Disposable Email Services

谢谢大家！欢迎讨论交流~

清华大学网络科学与网络空间研究院

wch22@mails.tsinghua.edu.cn

分享人：王楚涵