

EN-Bypass: 针对邮件代发提醒机制的安全评估方法

袁静怡, 李子川, 彭国军

(武汉大学国家网络安全学院空天信息安全与可信计算教育部重点实验室, 湖北 武汉 430072)

摘要: 电子邮件是人们日常生活、工作中非常重要的通信手段, 往往被攻击者作为钓鱼攻击的入口, 而发件人伪造则是实现邮件钓鱼攻击的关键步骤。为防止发件人伪造攻击, 邮件厂商往往会部署 SPF、DKIM 和 DMARC 等邮件安全协议来验证发件人身份, 除此之外, 部分厂商会在前端添加代发提醒机制辅助用户判断邮件的真实来源, 以降低用户受到钓鱼邮件威胁的可能。但是业界并没有统一标准对代发提醒机制的实现进行规范, 各厂商的代发提醒机制实现各不相同, 其实现上能否有效防止发件人伪造攻击仍缺少测试和验证。对邮件服务厂商代发提醒机制进行研究, 旨在评估厂商邮件代发提醒机制的安全性, 消除攻击者绕过代发提醒机制实现发件人伪造的潜在安全威胁。对 10 个国内外邮件厂商进行调研, 其中有 7 个厂商部署了代发提醒机制。在测试基础上提出了一种新型发件人伪造攻击——EN-Bypass 攻击, 该攻击通过构造和变换邮件头中的 From 和 Sender 字段, 绕过邮件代发提醒机制以实现发件人伪造。为了自动化验证代发提醒机制的安全性和可靠性, 基于 EN-Bypass 攻击的思路实现了工具 EmailSenderChecker, 用于对厂商代发提醒机制进行自动化测试。实验结果表明, 7 个厂商的代发提醒机制均存在不同程度的安全漏洞, 攻击者通过构造特殊的邮件头部可以绕过代发提醒机制, 实现发件人伪造攻击。最后, 为了提高邮件服务的安全性, 就邮件厂商代发提醒机制存在的问题, 向邮件服务厂商提出了安全建议。

关键词: 电子邮件; 邮件安全; 发件人伪造; 安全扩展协议

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2023041

EN-Bypass: a security assessment method on e-mail user interface notification

YUAN Jingyi, LI Zichuan, PENG Guojun

Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education,
School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China

Abstract: Email plays an important role in people's daily communications, while also attracts the attention of hackers.

收稿日期: 2022-12-29; 修回日期: 2023-05-30

通信作者: 彭国军, guojpeng@whu.edu.cn

基金项目: 国家自然科学基金 (62172308, U1626107, 61972297, 62172144)

Foundation Item: The National Natural Science Foundation of China (62172308, U1626107, 61972297, 62172144)

引用格式: 袁静怡, 李子川, 彭国军. EN-Bypass: 针对邮件代发提醒机制的安全评估方法[J]. 网络与信息安全学报, 2023, 9(3): 90-101.

Citation Format: YUAN J Y, LI Z C, PENG G J. EN-Bypass: a security assessment method on email user interface notification[J]. Chinese Journal of Network and Information Security, 2023, 9(3): 90-101.

Email is frequently used in phishing attacks, with email sender spoofing being a key step. To prevent sender-spoofing attacks, email vendors often deploy email security protocols such as SPF, DKIM, and DMARC to verify the sender's identity. Moreover, some vendors add email UI notification mechanism on email clients to help users identify the real sender. However, there is no uniform standard in the implementation of the email UI notification mechanism, which varies among vendors. Whether the mechanism effectively prevents sender-spoofing attacks still needs verification. In this paper, the security evaluation of the email UI notification mechanism was studied to gain better understanding of its efficacy and to eventually protect users from sender-spoofing attacks. Ten world-famous email services were researched and evaluated, of which seven deployed the email UI notification mechanism. Consequently, a new type of sender-spoofing attack was proposed which was called EN-Bypass, aiming to bypass the email UI notification mechanism by forging the "From" and "Sender" fields in the email header. To verify the email UI notification mechanism's security and reliability, EmailSenderChecker was implemented, which can automatically evaluate the existence of the EN-Bypass attack. The result shows that all seven email service vendors suffer from EN-Bypass attack. Attackers could bypass the email UI notification mechanism by constructing special email headers and spoofing the sender. Finally, to improve the mail service security, three suggestions about the email UI notification mechanism were proposed for the mail service vendors.

Keywords: e-mail, e-mail security, sender spoofing, security extension protocol

0 引言

电子邮件在人们日常生活中不可或缺,虽然即时通信发展迅速,但是电子邮件在商务合作、重要信息通知等方面仍有不可替代的作用。鱼叉式钓鱼攻击往往会将电子邮件作为入口,通过邮件诱导受害者下载带恶意代码的附件或点击钓鱼网站链接,达到木马植入、获取受害者账号密码等目的。近年来,利用电子邮件进行网络诈骗的案件数量急剧增加,网络犯罪分子根据实际情况调整骗术,对公司和个人进行诈骗,给受害者带来了非常大的经济损失^[1]。

邮件发件人伪造是网络邮件钓鱼攻击中一个重要的步骤,攻击者通过对邮件头部进行篡改使得前端显示的发件人为攻击者想要伪造的发件人,从而降低收件人的警惕。简单邮件传输协议(SMTP, simple mail transfer protocol)是最基础的邮件传输协议,但是该协议没有对发件人身份进行验证。为了防止发件人伪造攻击,发件人策略框架(SPF, sender policy framework)^[2],域名密钥识别邮件(DKIM, domainkeys identified mail)^[3]和基于域的邮件验证、报告和一致性(DMARC, domain-based message authentication, reporting & conformance)^[4]等协议被提出,用于验证邮件发件者身份^[5]。

近几年,邮件发件人伪造以及 SPF、DKIM 和 DMARC 等邮件安全协议的相关研究较多,由于邮件组件之间的不一致性或厂商安全协议部署存在问题,邮件发件人伪造攻击依旧存在。2018 年, Hu 等^[6]通过端到端的发件人伪造对邮件服务厂商 SPF、DKIM 和 DMARC 的部署情况进行评估,实验结果表明大多数邮件厂商没有配置安全协议或协议配置不当。尚菁菁等^[7]对国内外的政府机构的邮件安全协议部署进行了分析,发现部署 SPF 协议的政府机构约占 70%,部署 DMARC 协议的机构不足 30%,并且其中大部分部署 DMARC 协议的机构并没有配置严格的策略来阻止 SPF、DKIM 检测失败的邮件进入邮箱。Chen^[8]等工作表明,即使邮件服务厂商部署了 SPF、DKIM 和 DMARC 等安全协议,攻击者可以利用组件之间的不一致性,如邮件服务器进行安全检查的 From 和邮件客户端前端显示的 From 不一致、不同邮件服务厂商之间的验证机制和前端显示存在差异等,绕过安全协议实现发件人伪造攻击。Shen 等^[9]从邮件的发送验证、接收验证、转发验证和用户界面(UI, user interface)渲染 4 个环节对邮件安全进行研究,发现邮件服务厂商对安全协议的理解存在差异,并且在部署安全机制时存在问题,导致发件人伪造攻击依旧存在。

随着以上问题的提出,邮件服务厂商逐渐意识到邮件服务存在许多安全问题,邮件安全逐渐得到重视。2021年,Deccio等^[10]对大量邮件服务器的SPF、DKIM和DMARC部署情况进行研究,研究结果表明电子邮件安全协议部署范围相较之前更广泛,邮件安全性得到明显提升。本文对Chen^[8]和Shen^[9]提到的安全问题进行复现,发现大部分问题都已经被修复,并且很多厂商使用自研的安全机制来保障邮件的安全性。例如,部分厂商部署了代发提醒机制,该机制在检测到邮件声称的发件人与真实发件人不一致时,会在邮件客户端的UI界面显示标识或提醒语句,以提高用户警惕。Shen等^[9]将通过前端指示符提醒用户真实发件人和前端显示发件人不一致的机制称为发件人不一致检查(SIC, sender inconsistency check),本文将这一机制称为代发提醒机制,并在实践过程中发现目前缺少相关协议对代发提醒机制进行规范,不同邮件服务厂商的实现方法不同,可能存在安全性问题。

本文对10个国内外邮件厂商的代发提醒机制部署和实现情况进行调研,发现所有邮件厂商的代发提醒机制都存在问题,对这一问题进行了细致的研究,并提出了邮件用户界面提醒绕过(EN-Bypass, e-mail user interface notification bypass)攻击。EN-Bypass攻击能够绕过厂商的代发提醒机制。本文主要贡献如下。

1) 对10个国内外邮件服务商的From字段一致性检查策略的部署情况进行调研,并通过黑盒测试的方法对其实现原理进行分析。

2) 构建威胁模型,总结归纳出一种新型的邮件发件人伪造攻击,EN-Bypass攻击通过绕过邮件服务厂商代发提醒,实现发件人伪造攻击。

3) 实现了自动化完成EN-Bypass攻击的工具——EmailSenderChecker,并使用该工具对7个部署了代发提醒机制的厂商进行测试,发现所有厂商的代发提醒机制都存在安全漏洞。

1 背景

1.1 邮件头标识

电子邮件的头部中与发件人相关的字段主要有4个: Mail From(5321.MailFrom)、Return-Path、

From(5322.From)和Sender。

Mail From 字段被称为“信封发件人”或“5321.MailFrom”, Mail From 在SMTP传输中用于标识发件人,同时被当作返回路径(Return-Path)地址,该字段不会在邮件客户端显示。

Return-Path 字段用于标识邮件的返回地址,当邮件投递失败或者邮件系统出现故障时,错误报告将会发送到 Return-Path 指定的地址。RFC 5321 中明确指出发送邮件的SMTP系统不应该发送邮件头中已经包含 Return-Path 字段的邮件,并且接收邮件的SMTP系统可以删除邮件头中的 Return-Path 字段,自己添加新的 Return-Path^[11]。

From 字段被称为“信头发件人”或“5322.From”,该字段标识了邮件的作者,也是邮件客户端会显示在UI界面上的发件人。

Sender 字段指定了实际负责传输邮件的代理邮箱地址,如果邮件的作者和传递者相同,则不需要Sender字段。Chen等^[8]指出在From字段缺失的情况下,部分邮件服务提供商在UI界面上显示Sender字段为发件人;RFC 5322规定如果From字段中包含多个地址,则Sender必须在邮件头中出现^[12]。

1.2 邮件安全扩展协议

SMTP设计时没有考虑邮件的安全性。为了保证电子邮件的完整性和可靠性,邮件安全扩展协议被相继提出,其中SPF、DKIM和DMARC协议是目前使用最广泛的3种邮件安全扩展协议。

SPF协议先查询信封发件人的邮箱域名对应的SPF记录,再通过判断发件人IP是否在该记录中来确定邮件的安全性。

DKIM协议一般使用邮件发送域的私钥对邮件进行签名,并将生成的DKIM签名添加到邮件头中,接收方通过该签名验证邮件的完整性。该协议除了防止发件人伪造外还可以保证邮件的完整性。

DMARC协议以SPF和DKIM两者认证结果为基础,再对邮件头中的From字段进行对齐检查。DMARC允许域名所有者发布“失败策略”,该策略决定了收件服务器如何处理校验不通过的邮件。

1.3 From 字段一致性检查

邮件安全扩展协议中 SPF 对 Mail From 字段进行验证, DKIM 对签名域进行验证, DMARC 协议会进一步对 From 字段的域名进行标识符对齐检查。本文调研了国内外多个邮件厂商的安全机制, 将 From 字段一致性检查的策略总结概括为以下 4 种类型。

1) 发件检查: 邮件发件 SMTP 服务器对 From 字段和 Mail From 字段进行一致性检查, 如果不匹配, 可能导致发件失败。

2) 收件检查: 邮件收件 SMTP 服务器对 From 字段进行检查, 如果 From 和 Mail From 字段不一致则退信。

3) DMARC 对齐检查: 邮件接收 SMTP 服务器对 From 进行 DMARC 的标识符对齐检查。

DMARC 的标识符对齐机制通过检查 From 的域名、SPF 验证时使用的域名以及 DKIM 签名域的一致性来判断邮件安全性。对齐机制分为严格模式和宽松模式, 严格模式要求域名完全相同, 宽松模式只需要组织域相同。如果邮件未通过 DMARC 检查, 邮件接收服务器会查询 From 字段的域名对应的 DMARC 策略, 该策略中包含校验失败时对邮件的处理方式——拒收邮件、将邮件投入垃圾箱和不做处理。

4) 代发提醒: 代发提醒机制用于在 UI 界面中提醒用户显示的发件人可能并非邮件的真实发件人。目前没有明确的安全协议对邮件客户端的代发提醒机制进行规范, 各邮件服务厂商实现方法不同。

图 1 展示了邮件传递过程中 4 种会对 From 字段进行一致性检查的策略。

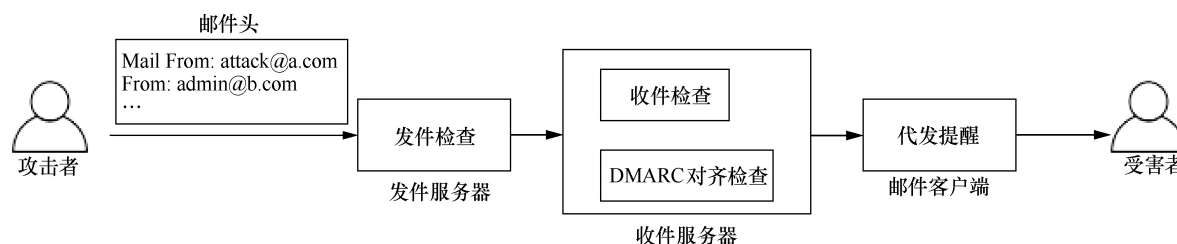


图 1 From 字段一致性检查
Figure 1 Consistency checks for From

1.4 发件人伪造攻击

发件人伪造攻击被用于网络钓鱼攻击, 攻击者通过对邮件头部进行伪造, 使邮件客户端显示的发件人和真实发件人不一致, 降低用户的警惕, 诱导用户点击恶意链接或者下载带有恶意软件的附件。

本文定义成功的发件人伪造攻击需要同时满足以下 3 个条件: ① 邮件进入收件箱; ② 收件人邮件 Web 客户端显示发件人为攻击者伪造的发件人; ③ 界面不显示代发提醒。

2 厂商安全性测试

本文选取在国内开放注册的 10 个邮件厂商进行测试, 为保护厂商隐私, 本文对厂商进行匿名化处理, 其中 A、B、H 和 J 为国外邮件厂商, C、D、E、F、G、I 为国内邮件厂商。本节对 10 个邮件厂商的 From 字段一致性检查策略部署情况进行测试。本文通过发送批量邮件对各个厂商发

件检查、收件检查、DMARC 对齐检查和代发提醒的部署情况进行测试, 安全检查情况如表 1 所示, “√”为部署该检查机制, “×”为没有部署该检查机制。因为厂商 J 没有提供免费的 SMTP 服务, 所以发件检查一栏为“—”。

本文使用 4 封邮件来对厂商发件检查情况进行测试, 假设待测试邮箱为 test1@a.com, From 字段篡改为 any@a.com 或 any@b.com, 收件人为 test2@a.com 或 test2@b.com, From 字段和收件人选取不同的邮箱地址排列组合产生 4 封测试邮件。如果 4 封邮件均可成功发送, 则认为厂商没有进行严格发件检查。结果表明, 10 个厂商中 6 个厂商部署了发件检查。其中, 国外厂商 B 同时会对 Sender 和 From 两个字段进行检查, 如果这两个字段任意一个和 SMTP 服务认证的邮箱不一致, 则会发件失败。国内厂商 G 对域内发件的情况会进行严格发件检查, 当收件人为厂商 G 的用户时, From 字段和 Mail From 不一致, 则会发件

失败；但是当收件人为其他厂商邮箱，则不会进行发件检查。厂商 F 和 G 则是要求 From 字段和 Mail From 字段一致，否则发件失败。厂商 I 虽然能顺利完成 SMTP 会话，但是 SMTP 发件服务器会将伪造 From 字段的邮件退回。厂商 A 比较特殊，虽然 From 字段和 Mail From 字段不一致时可以发件成功，但是 SMTP 发件服务器在发送邮件时会将从修改为真实发件人，并用“X-A-Original-From”字段记录原 From 字段。其余邮箱可成功发送 4 封测试邮件。

收件检查的测试和发件检查类似，这里将 test1@a.com 设置为待测试邮箱，然后使用 test2@a.com 或 test2@b.com 进行发件，From 字段篡改为 any@a.com 或 any@b.com。通过退信情况来评估厂商的收件检查。测试结果表明，国外厂商 B 会将 From 字段伪造成来自厂商 B 域的邮件退信。国外厂商 J 不会在收件箱或垃圾箱中显示 From 字段伪造成来自厂商 J 域的邮件，但是发件邮箱也没有收到退信通知。

DMARC 对齐检查的测试比较特别，因为部分邮件厂商邮件头部并没有显示 DMARC 校验结果，所以无法通过查看邮件头的方法来判断厂商是否进行了 DMARC 检查。当对厂商进行测试时，首先将 test@a.com 设置为收件人，然后使用 test@b.com 进行发件，同时 From 字段伪造成 any@c.com，这种情况下 DMARC 校验是失败的。这里挑选域名 DMARC 失败策略为拒绝的邮箱作为 any@c.com，进行 DMARC 检查的收件服务器在邮件 DMARC 校验失败时，会按照 DMARC 策略对邮件进行退信处理。如果邮件被退回或邮件头部显示 DMARC 校验结果，则认为厂商进行了 DMARC 对齐检查，否则认为厂商没有部署相关策略。测试结果表明，厂商 A、G、H 和 J 进行了 DMARC 对齐检查。其中厂商 A 和 G 退回了邮件。厂商 B 会在前端提醒用户邮件 DMARC 校验失败。厂商 H 和 J 虽然接收了邮件，但是邮件被投入垃圾箱，并且 DMARC 校验结果为“Fail”。其余厂商并没有执行退信操作，并且邮件头部也没有 DMARC 校验信息，本文认为这些厂商没有对邮件进行 DMARC 对齐检查。

表 1 From 字段安全检查情况

Table 1 The results of From filed security check

邮件服务 厂商	发件 检查	收件 检查	DMARC 对齐检查	代发 提醒
国外厂商 A	✓	×	✓	✓
国外厂商 B	✓	✓	✓	✓
国内厂商 C	×	×	×	✓
国内厂商 D	×	×	×	✓
国内厂商 E	×	×	×	✓
国内厂商 F	✓	×	×	✓
国内厂商 G	✓	×	✓	✓
国外厂商 H	✓	×	✓	×
国内厂商 I	✓	×	×	×
国外厂商 J	—	✓	✓	×

图 2 为某厂商的代发提醒机制，各个邮件厂商的代发提醒样式不同，但都是为了辅助用户识别邮件真实发件人，从而降低发件人伪造攻击成功率。

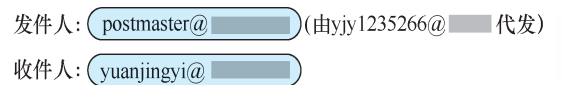


图 2 代发提醒
Figure 2 Sender notification

本文通过发送多封伪造邮件来测试厂商是否部署代发提醒机制，测试结果表明除了厂商 H、I 和 J 未部署代发提醒外，其余厂商均部署了代发提醒。

通过对邮件头的分析，发现邮件代发提醒机制通常使用 From 字段和 Sender 字段或 From 字段和 Return-Path 字段进行一致性匹配来保证 From 字段的准确性。厂商 C、D、E、F、G 通过检查 From 字段和 Sender 字段是否一致来判断发件人的真实性，如果 From 字段和 Sender 字段不一致，则在 UI 界面显示代发。厂商 B 则使用 Return-Path 字段来进行对比。

为了进一步对厂商代发提醒机制的安全性进行测试，本文尝试篡改邮件的 Sender 字段和 Return-Path 字段。测试结果表明，Sender 字段可以被篡改成功，但是 Return-Path 往往被覆盖或者删除。结合 RFC 5321 标准中的相关规定和具体实验，发现使用 Return-Path 对 From 进行一致性检查的邮件服务厂商在接收邮件时会添加新的

Return-Path 或者直接覆盖邮件头中已存在的 Return-Path, Return-Path 字段难以被攻击者控制。但是 Sender 字段可以被更改, 如果厂商没有对 Sender 字段进行保护, 且使用 Sender 字段和 From 字段进行一致性匹配, 则其代发提醒机制可能存在安全性问题。

3 威胁模型

3.1 EN-Bypass 攻击

本文的研究重点在于邮件服务厂商代发提醒机制中存在的问题, 并将绕过邮件客户端 UI 界面代发提醒的一类问题统称为 EN-Bypass 攻击。

之前关于邮件发件人伪造的研究工作主要是对 From 和 Mail From 进行篡改实现发件人伪造攻击, 并没有过多关注 Sender 和 Return-Path 对邮件安全带来的影响。本文通过对邮件头部中的 Sender 和 Return-Path 进行篡改来绕过邮件服务厂商的代发提醒, 使邮件客户端显示的发件人为被伪造发件人, 且不出现代发提醒。

结合第2节对厂商安全性测试的实验, 发现 Return-Path 字段难以被控制, 但是 Sender 字段可以被篡改。本文选择对 Sender 进行篡改, 实现 EN-Bypass 攻击。

3.2 条件假设

本节根据攻击目的和攻击者能力的不同来对攻击类型进行分类。

(1) 攻击目的

本文将攻击者希望在前端显示的发件人称为被伪造发件人, 这里将被伪造发件人划分为两类。

1) 被伪造发件人和攻击者的邮箱域名相同。DMARC 协议对 From 字段的域名进行对齐检查, 而非 From 字段本身, 当攻击者将“hacker@a.com”伪造成“admin@a.com”时, DMARC 检查是通过的。

2) 被伪造发件人和攻击者的邮箱域名不同。这种情况下 DMARC 的对齐检查不通过, 收件服务器的处理方法由被伪造发件人的域名对应的 DMARC 策略决定。

(2) 攻击者能力

根据攻击者的能力, 将攻击者分为两类。

1) 攻击者使用和受害者(收件人)相同域名的邮箱进行发件。这种情况常见于受害者使用的是公开注册的邮箱, 本文将真实发件人和收件人在同一域的情况称为域内发件。这种情况下攻击者为域内发件, 如果邮件厂商对于域内发件没有进行严格的安全检查则会存在安全问题。

2) 攻击者发件邮箱与收件人邮箱域名不同。当收件人邮箱为企业邮箱、内部邮箱时, 攻击者可能无法注册到与受害者相同域名的邮箱, 这种情况下攻击者是跨域发件, 邮件收件服务器通常会对邮件进行 SPF、DKIM 和 DMARC 等安全检查。

3.3 攻击类型

本节将 3.2 节中提出的条件假设进行排列组合, 得到以下 4 种攻击类型, 图 3 为攻击类型的示意。

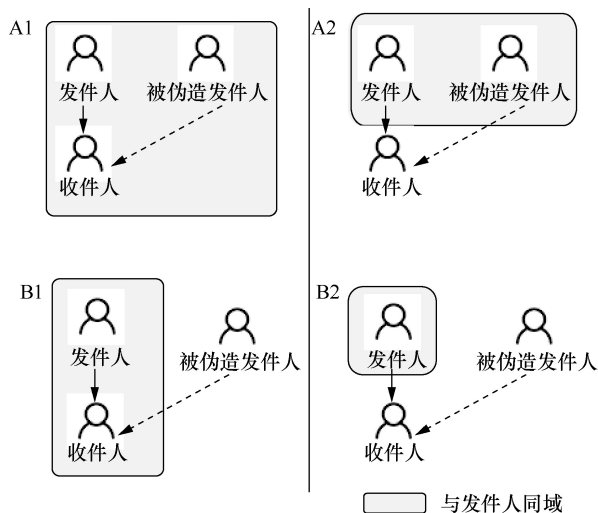


图3 攻击类型示意
Figure 3 Attack types diagrams

A1: 攻击者、收件人以及被伪造发件人都在同一个域内; 这种攻击类型下攻击者和被伪造发件人同域, 所以 DMARC 检查是通过的, 但是攻击者需要注册到受害者域名下的邮箱。

A2: 被伪造发件人与攻击者同域, 收件人与攻击者不同域; A2 情况与 A1 类似, DMARC 对 From 的域名对齐检查是通过的, 同时攻击者可以使用任意邮箱发件。

B1: 被伪造发件人与攻击者不同域, 攻击者和收件人同域; 攻击者和被伪造发件人不同域, DMARC 校验为失败, 攻击者和收件人同域, 需

要注册到和受害者相同域名的邮箱。

B2: 攻击者、发件人及被伪造发件人不同域; 这种情况下 DMARC 对齐检查是失败的, 攻击者可以选取任意邮箱发件, 被伪造发件人为其他域邮箱。

表 2 给出每种攻击类型的攻击场景。

表 2 攻击场景
Table 2 Attack scenarios

攻击类型	攻击者-被伪造发件人	攻击者-收件人	攻击场景示例
A1	同域伪造	域内发件	攻击者、收件人都拥有同一厂商的邮箱, 攻击者伪装为邮箱管理员, 向收件人发送带有钓鱼链接的邮件
A2	同域伪造	跨域发件	适用于受害人(收件人)邮箱为企业内部邮箱的攻击场景, 攻击者将发件人伪装成发件域内收件人信任的用户, 对收件人进行欺骗
B1	跨域伪造	域内发件	攻击者将邮箱伪装成某公司人力资源部门或政府机构的官方邮箱对收件人进行钓鱼或诈骗
B2	跨域伪造	跨域发件	攻击者与收件人不在同一域, 攻击者将自己的邮箱伪装成其他域任意邮箱或收件人域内的其他用户。例如, 攻击者伪造成企业内部高管, 向该企业的员工发送包含恶意附件的邮件

3.4 攻击方法

通过对攻击类型的分析, 本节归纳出如下两种攻击方式。

1) 直接对 From 进行伪造: 将 From 直接设置为被伪造发件人, 如果厂商在 DMARC 通过的情况下不会再对 From 进行安全检查, 则发件人伪造攻击成功。

2) 同时对 From 和 Sender 进行伪造: 将 From 设置为被伪造发件人, 此外还要对 Sender 进行篡改, 用于绕过代发提醒。

4 系统实现

EN-Bypass 攻击通过发送带有特殊头部的邮件实现发件人伪造, 如果邮件成功进入收件箱, 前端显示发件人为被伪造发件人, 并且没有代发提醒, 则发件人伪造攻击成功。如果直接将 Sender 字段设置为被伪造发件人, 则邮件收件服务器会对 Sender 字段进行修正, 将其设置为真实发件人。所以, 直接伪造的方法无法实现发件人伪造攻击, 需要对 Sender 字段进行变异, 干扰收件服务器对其的解析, 使 Sender 字段能通过和 From 字段的一致性匹配。但是通过人工的方法构造使收件服务器解析出错的 Sender 字段难度较大。图 4 为绕过某厂商代发提醒机制的有效载荷, 该邮件头中包含两个 Sender 字段, 且均设置为空, 人工查看时两个 Sender 字段相同, 但实际上第一个 Sender 字段末尾包含一个空格, 而第二个 Sender 字段不包含空格。此类攻击载荷往往难以通过人工获得, 本文设计 EmailSenderChecker 工具通过自动化构造特殊的 Sender 字段对多个厂商代发提醒机制进行安全性评估。

邮件头

```

From: postmaster@xxx.com
Sender: <> 
Sender: <> 
To: victim@xxx.com
  
```

图 4 攻击有效载荷实例
Figure 4 Attack case of payload

4.1 EmailSenderChecker 设计

EmailSenderChecker 将 EN-Bypass 攻击和攻击效果检测的过程自动化, EmailSenderChecker 包含两个功能: 预测试功能和自动化测试功能。

图 5 为 EmailSenderChecker 的架构, 其中蓝

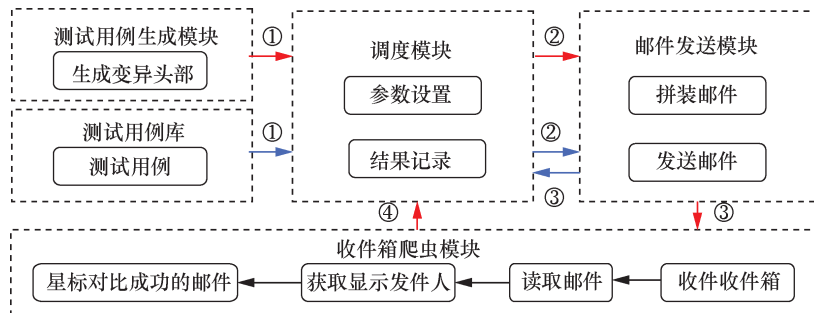


图 5 EmailSenderChecker 的架构
Figure 5 The architecture of EmailSenderChecker

色表示预测试流程, 红色表示自动化测试流程, 预测试将第2节中测试厂商安全策略部署情况的过程半自动化, 本文将手动测试时使用到的测试邮件模板化, 预测试模块直接自动发送相关测试邮件, 然后人工分析收件结果, 了解厂商安全策略部署情况。预测试功能可以了解厂商的SMTP服务器的发件检查策略、收件客户端是否设置代发提醒、代发提醒策略检查的字段、DMARC对齐检查情况。根据预测试结果可以对发件时间间隔、被伪造发件人等参数进行适当的调整, 提高自动化测试效率。

自动化测试功能通过发送带有特殊头部的邮件, 再使用爬虫模块自动化检测EN-Bypass攻击效果来判断被测试邮箱是否存在漏洞。自动化测试中包含两个重要的模块: 测试用例生成模块和收件箱爬虫模块。测试用例生成模块生成伪造的From字段和变异的Sender字段, 通过发件模块将带有特殊头部的邮件发送给被测试邮箱。收件箱爬虫模块用于自动化检测攻击结果, 爬虫对进入收件箱的邮件进行检查, 使用XPath解析提取UI界面显示的发件人字段, 然后将该字段与EN-Bypass攻击的预期结果进行对比, 如果攻击成功, 则星标邮件, 并将种子返回到调度模块中。

EmailSenderChecker包括测试用例生成模块、邮件发送模块、收件箱爬虫模块和调度模块。下面将对每一个模块进行详细介绍。

4.2 测试用例生成模块

EN-Bypass攻击的攻击方法包括两类: ①对From字段进行伪造; ②对From和Sender字段同时进行伪造。这里给出From字段和Sender字段的伪造方法。

电子邮件消息格式标准最早在RFC 822中定义, 之后通过RFC 2822、RFC 5322和RFC 6854逐步更新。From字段和Sender字段都是由邮箱构成的, 邮箱主要由两部分组成。①显示名称: 显示名称是一个可选字段, 用于在邮件应用程序中显示的发件人。②地址: 用尖括号("<"和">")包围起来的邮箱地址。此外, 邮箱也可以由简单的地址构成, 不需要显示名称和尖括号。

这里直接将From伪造成被伪造发件人, 即直接伪造。将From设置为被伪造发件人, From:

display-name <spoof-sender@a.com> 或 From: spoof-sender@a.com。

在观察正常邮件信头时发现, Sender中通常没有显示名称, 而是直接由地址构成, 所以在对Sender进行变异时不考虑显示名称, 只考虑地址。

1) 直接伪造: 将邮箱地址设置为被伪造发件人, Sender: <spoof-sender@a.com> 或 Sender: spoof-sender@a.com。

2) 多个地址: 将真实发件人地址和被伪造发件人地址都放入Sender中, 如 Sender: spoof-sender@a.com real-sender@b.com, 干扰收件服务器对Sender字段的正确解析。

3) 将地址置空: 将邮箱地址置为空, Sender: <> 或 Sender:, 看邮件服务器能否正常处理Sender为空的情况。

4) 插入特殊字符: 通过在多个地址之间插入诸如“\”“\n”和“,”等特殊字符, 对邮箱地址进行截断。

5) 相同字段重复多次: 本条变异策略指将Sender字段重复多次, 收件服务器可能使用不同的Sender字段进行安全检查。

6) 多种变异策略组合: 对上述变异策略进行排列组合生成新的变异规则。

4.3 邮件发送模块

邮件发送模块将邮件头部和邮件体拼接, 然后将邮件发送到需要测试的目标邮箱。该模块将变异策略生成的From、Sender字段添加到邮件头中, 邮件头中的收件人(To)、返回路径(Return-Path)等其他字段不做修改。

为了减少邮件服务商的垃圾邮件检测机制对实验结果产生影响, 尽量避免邮件因为内容被投入垃圾箱的情况, 所以邮件体中填充的内容是正常的邮件内容, 不包含任何恶意信息。

Hu^[6]、Shen^[9]等选用10 min一封邮件的频率对邮件服务器进行测试, 从而避免对测试的邮件服务器产生影响。本文在测试时会用到不同邮件厂商的SMTP服务, 不同厂商提供给用户的SMTP服务对每日发件上限规定不同, 具体发件频率可以根据邮件服务厂商官方的SMTP服务发件限制来进行调整, 在不影响被测试的邮件服务

器的情况下,可以适当提高发件频率以提高测试效率。本文在测试中使用较多的发件频率为3 min一封。

4.4 收件箱爬虫模块

本文对邮件厂商的邮件 Web 客户端进行测试,当邮件发送之后,需要检查被测试邮箱的收件箱来判断 EN-Bypass 攻击是否成功。收件箱爬虫模块通过模拟真实用户的操作,检查最新收到的邮件,解析提取邮件客户端 UI 显示的发件人,并将 UI 显示的发件人与预期结果进行对比来判断 EN-Bypass 攻击是否成功。该模块使用 Selenium 模拟用户登录、查看收件箱的操作,使用 XPath 提取 UI 显示发件人。

收件箱爬虫模块提供两种登录被测邮箱的方式:普通登录模式和 Cookie 登录模式。普通登录模式下爬虫需要模拟用户登录,只需要为爬虫模块设置邮箱的用户名和密码。安全性较高的邮件服务厂商会在邮箱登录的过程中设置人机验证,如国外厂商 A 登录时需要输入验证码,这里通过给 Selenium WebDriver 添加 Cookie 来绕过人机验证。Cookie 登录模式下需要人工获取 Cookie 之后添加给爬虫模块,设置完 Cookie 之后爬虫可以直接进入用户界面。

收件箱爬虫模块需要为邮件客户端 Web 页面创建定制的 XPath 选择器,来解析页面中有价值的元素。该模块仅关注进入收件箱的邮件,对于进入收件箱的邮件,爬虫通过 XPath 得到 UI 界面中显示的发件人,通过与被伪造发件人匹配来判断伪造是否成功,之后检测是否出现代发提醒。当 UI 界面显示的发件人为被伪造发件人且没有显示代发提醒时,爬虫判断 EN-Bypass 攻击成功,并将邮件进行标记。成功实现 EN-Bypass 攻击的变异头部会被返回给调度模块,攻击成功的种子会在其他邮箱的预测试过程中使用。

如果邮件进入垃圾箱,可能是 DMARC 验证不通过导致的,进入垃圾邮箱的邮件被判定为 EN-Bypass 攻击失败,不进行关注。对于收件箱中没有收到邮件的情况,可能是网络问题导致发送失败或是未通过收件 SMTP 的检测导致退信,为了避免网络问题导致误差,调度模块会重发未

收到的邮件。

4.5 调度模块

调度模块的主要功能是任务调度以及设置重要的参数。通过调度模块选择执行预测试功能或自动化测试功能。调度模块中需要设置的参数包括被伪造发件人、被测试邮箱、发件邮箱、发件频率等。调度模块还需要处理测试返回的结果,如保存攻击成功的种子。

5 实验与评估

本文使用 EmailSenderChecker 对部署代发提醒机制的7个邮件厂商进行 EN-Bypass 攻击,并统计、分析测试结果。前文将攻击类型划分为4类,为了更直观概括这4类攻击,本文使用同域伪造和跨域伪造来描述攻击者与被伪造发件人之间的关系,使用域内发件和跨域发件来描述攻击者与收件人的关系,如 A2 类型为被伪造发件人与攻击者同域,攻击者和收件人不同域,这里简称为同域伪造-跨域发件攻击。按此规则4种攻击类型分别命名为: A1 (同域伪造-域内发件攻击)、A2 (同域伪造-跨域发件攻击)、B1 (跨域伪造-域内发件攻击)和 B2 (跨域伪造-跨域发件攻击)。

5.1 实验结果

本文对部署代发提醒机制的7个邮件厂商的 Web 客户端进行测试,表3为具体实验结果,“√”代表存在该类型的漏洞,“×”为未检测到该类型漏洞。

通过测试发现厂商 A 和 B 存在 A2 型漏洞,厂商 C、D、E 存在 A1 和 A2 型漏洞,厂商 F 和 G 存在 A2 和 B2 型漏洞。

厂商 A 和 B 存在 A2 型漏洞。对 A 和 B 而言,代发提醒是对 DMARC 校验失败的补充验证,提醒用户邮件可能来自别的域名。A2 型攻击要求攻击者和被伪造发件人同域,在这种情况下,SPF、DKIM 和 DMARC 这3个安全协议都是通过的,但是 DMARC 只对 From 的域名进行检查,不能保证 From 字段本身的准确性。

本文发现厂商 C、D 和 E 存在 A1、B1 型问题。这3个邮件服务厂商在接收到邮件后对 From 和 Sender 进行一致性匹配,如果二者不一致,则会在前端显示代发提醒。存在 A1、B1 型漏洞意味着如果攻击者拥有该邮件厂商的合法邮

箱, 则攻击者可以在域内发件的情况下, 伪造任意发件人。

厂商 F 和 G 存在 A2、B2 型漏洞。厂商 F 在检测到 Sender 和 From 不一致时会显示代发提醒, 但是厂商 F 的代发提醒可以直接通过修改 Sender 进行绕过, 从而实现 A2、B2 型攻击。在测试厂商 F 的 B2 型漏洞时, 当将被伪造发件人设置为该厂商的用户时, 邮件被直接投入垃圾箱。

结合表 1 中厂商 From 字段检查的部署情况和表 3 的代发提醒机制测试结果发现: 存在 A2 (同域伪造-跨域发件攻击) 型攻击的邮件服务厂商, 如 A、B 等, 这些邮件服务商提供的 SMTP 服务在发件前会进行严格的发件检查, From 与 Mail From 一致才能成功发件。所以, 攻击者无法通过这些厂商的 SMTP 服务发送伪造邮件, 实现 A1、B1 型攻击。但是这些厂商忽略了其他厂商的 SMTP 服务可能存在发件检查不严格的情况, 没有对 DMARC 校验通过的邮件进行进一步检查 (厂商 A、B) 或代发提醒机制存在问题 (厂商 F、G), 导致 A2 型攻击存在; 而厂商 C、D 和 E 的邮件服务商对 SMTP 服务的发件检查并不严格, From 字段与真实发件人不一致的情况下也能成功发件, 虽然这些厂商部署了代发提醒机制, 但是这些厂商的代发提醒机制均存在漏洞, 在域内发件时攻击者可以通过篡改 Sender 字段绕过代发提醒机制, 从而实现 A1、B1 型攻击。

表 3 EmailSenderChecker 实验结果
Table 3 The test results of EmailSenderChecker

邮件服务厂商	A1 (同域伪造-域内发件)	A2 (同域伪造-跨域发件)	B1 (跨域伪造-域内发件)	B2 (跨域伪造-跨域发件)
国外厂商 A	×	√	×	×
国外厂商 B	×	√	×	×
国内厂商 C	√	×	√	×
国内厂商 D	√	×	√	×
国内厂商 E	√	×	√	×
国内厂商 F	×	√	×	√
国内厂商 G	×	√	×	√

5.2 EmailSenderChecker 工具评估

为了验证 EmailSenderChecker 对邮件系统漏洞的检测效率和测试用例模块生成的种子的有效性, 本文设计了两个实验对工具的效果进行评估。

(1) 漏洞检测效率

本文通过 EmailSenderChecker 检测出邮件服务厂商单种漏洞的时间来对其效率进行评估, 表 4 为具体测试结果。

表 4 EmailSenderChecker 漏洞检测效率
Table 4 Detection efficiency of EmailSenderChecker

邮件服务厂商	漏洞类型	攻击方法	时间/s
国外厂商 A	A2	伪造 From	—
国外厂商 B	A2	伪造 From	—
国内厂商 C	A1.B1	伪造 From 和 Sender	186
国内厂商 D	A1.B1	伪造 From 和 Sender	63
国内厂商 E	A1.B1	伪造 From 和 Sender	53
国内厂商 F	A2.B2	伪造 From 和 Sender	32
国内厂商 G	A2.B2	伪造 From	—

因为仅伪造 From 的攻击方法比较简单, 只需要一封邮件即可完成, 不便进行计时统计, 所以时间一栏为“—”。同时, 对 From 和 Sender 进行伪造的攻击方法通常需要多封邮件进行测试, 本文使用最短的发件间隔来进行实验, 即 Email SenderChecker 完成前一封邮件的前端检查后立即发送下一封邮件。测试结果表明, EmailSender Checker 可以在较短的时间内检测出厂商存在的漏洞。

(2) 种子有效性

为了评估变异策略的有效性, 本文对工具生成的种子有效性进行评估, 这里将能成功实现发件人伪造攻击的种子称为有效种子。EmailSenderChecker 的测试用例生成模块共生成 426 个种子, 本文在厂商 C 和 D 上对这些种子进行测试, 结果如表 5 所示。结果表明, 426 个种子中有 50 个能实现对厂商 C 的邮件系统的攻击, 184 个实现对厂商 D 的邮件系统的攻击, 种子命中率, 能更快地完成邮件系统漏洞的检测。

5.3 案例分析

图 6 为厂商 D 的 A1、B1 型攻击实例, 攻击者拥有该厂商的合法邮箱, 想要欺骗该厂商中其他的邮箱用户, 该场景下攻击者使用厂商提供的

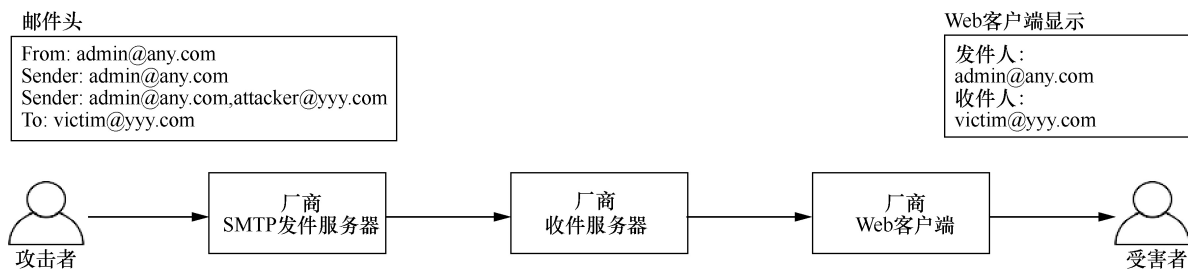


图 6 攻击实例
Figure 6 Attack case

SMTP 服务进行发件。攻击者先将 From 直接设置成被伪造发件人，再在邮件头中加入两个 Sender 字段。该邮件在邮箱 Web 客户端显示的发件人为被伪造发件人，并且不显示代发，发件人伪造攻击成功。

表 5 种子有效性
Table 5 Availability of seeds

邮件服务厂商	有效种子数	命中率
国内厂商 C	50	11.74%
国内厂商 D	184	43.19%

在第 2 节的测试中，已知该厂商没有对邮件进行 DMARC 对齐检查，只对 From 和 Sender 进行一致性检查，如果不匹配，则显示代发提醒。该厂商并非没有对 Sender 进行保护，当只设置一个 Sender 字段（设置为“admin@ any.com”或“admin@any.com, attacker@ yyy.com”）发送邮件，在收件箱查看邮件源发现 Sender 被修改回“attacker@yyy.com”，并且在前端显示代发提醒。本文推测该厂商在接收到邮件时会 对 Sender 和 Mail From 进行一致性检查，如果不匹配，则将 Sender 设置为 Mail From。但是在有多个 Sender 字段的情况下，服务器将第一个 Sender 字段修改为 Mail From，第二个 Sender 字段保留。第二个字段中“admin@any.com, attacker@yyy.com”被“,”截断，使用“admin@any.com”和 From 字段进行匹配。

5.4 安全建议

本节对邮件服务提供商提出以下几点安全建议。

1) 提供 SMTP 服务的厂商应该做好发件检查，厂商不应该允许 From 和 Mail From 不一致的邮件发件成功。

2) 如果厂商使用 Sender 来判断 From 字段的真实性，则需要增加对 Sender 字段的保护。

3) DMARC 协议只验证 From 字段域名的准确性，无法保证 From 为真实发件人，所以厂商需要额外对 From 进行一致性检查。

6 结束语

本文提出了绕过代发提醒的 EN-Bypass 攻击，通过对 Sender 进行变异实现发件人伪造攻击。邮件服务厂商可以根据所提出的 EN-Bypass 这 4 种攻击类型对自己的邮件服务进行安全性测试。

本文对 10 个国内外邮件厂商进行调研，发现 7 个厂商部署了代发提醒机制，使用 Email SenderChecker 对部署代发提醒的厂商进行 EN-Bypass 攻击检测，发现这 7 个邮件厂商都存在一定的安全问题。本文测试发现的漏洞均已上报厂商，部分厂商已修复相关漏洞。

通过实验发现，对 SMTP 服务进行严格发件检查的邮件服务厂商，会在发件过程中检查 From 和 Mail From 是否一致，如果不一致，则会发件失败，所以攻击者无法使用这些厂商的合法邮箱进行发件人伪造攻击。但是这些厂商的代发提醒机制并不严格，接收到邮件之后没有对 From 字段进行严格的检查，所以可以利用 DMARC 协议仅对 From 域名进行对齐检查的特性实现发件人伪造攻击。

代发提醒严格的邮件服务厂商对 From 和 Sender 的一致性匹配比较严格，但是厂商没有对 Sender 字段进行很好的保护，导致攻击者通过在邮件头部添加特定的 Sender 字段，可以绕过代发提醒。并且这些厂商提供的 SMTP 服务发件检查并不严格，From 和 Mail From 不一致时邮件也可

以成功发送。

厂商在设计 and 实现发件、收件和前端显示的安全策略的过程中, 没有考虑到其他厂商的安全策略, 但是邮箱使用者收到的邮件来自不同的域名, 这些域名对应的服务厂商的安全策略各有不同, 邮件厂商安全策略之间的不一致导致邮件发件人伪造的问题依旧存在。

本文在研究过程中还发现一些其他的问题: 部分邮件厂商发件检查并非将 **From** 和 **Mail From** 进行严格的匹配, 而是通过构造特殊的 **From** 字段可能绕过发件检查; 此外, 很多邮件厂商的邮件头部中有一些特殊字段, 这些特殊字段应该是厂商自研的安全策略, 如果厂商没有对这些字段做比较好的保护, 则可能存在安全隐患。

参考文献:

- [1] AL-MUSIB N S, AL-SERHANI F M, HUMAYUN M, et al. Business email compromise (BEC) attacks[J]. *Materials Today: Proceedings*, 2021.
- [2] WONG M, SCHLITT W. Request for comments 7208, sender policy framework (SPF) for authorizing use of domains in email, version 1[S]. RFC Editor, 2006.
- [3] CROCKER D, HANSEN T, KUCHERAWY M. Request for comments 6376, Domainkeys identified mail (dkim) signatures[S]. RFC Editor, 2011.
- [4] KUCHERAWY M, ZWICKY E. Request for comments 7489, domain-based message authentication, reporting, and conformance (DMARC)[S]. RFC Editor, 2015.
- [5] HU H, PENG P, WANG G. Towards understanding the adoption of anti-spoofing protocols in email systems[C]//IEEE Secure Development Conference (SecDev). 2018: 94-101.
- [6] HU H, WANG G. End-to-end measurements of email spoofing attacks[C]//27th USENIX Security Symposium (USENIX Security 18). 2018: 1095-1112.
- [7] 尚菁菁, 朱宇佳, 刘庆云. 电子邮件安全扩展协议应用分析[J]. *网络与信息安全学报*, 2020, 6(6): 69-79.
SHANG J J, ZHU Y J, LIU Q Y. Analysis of security extension protocol in e-mail system[J]. *Chinese Journal of Network and Information Security*, 2020, 6(6): 69-79.

- [8] CHEN J, PAXSON V, JIANG J. Composition kills: a case study of email sender authentication[C]//29th USENIX Security Symposium (USENIX Security 20). 2020: 2183-2199.
- [9] SHEN K, WANG C, GUO M, et al. Weak links in authentication chains: a large-scale analysis of email sender spoofing attacks[C]//30th USENIX Security Symposium (USENIX Security 21). 2021: 3201-3217.
- [10] DECCIO C, YADAV T, BENNETT N, et al. Measuring email sender validation in the wild[C]//Proceedings of the 17th International Conference on Emerging Networking Experiments and Technologies. 2021: 230-242.
- [11] KLENSIN J. Request for comments 5321, simple mail transfer protocol[S]. RFC Editor, 2008.
- [12] RESNICK P. Request for comments 5322, Internet message format[S]. RFC Editor, 2008.

[作者简介]



袁静怡 (1998—), 女, 湖南常德人, 武汉大学硕士生, 主要研究方向为网络安全。



李子川 (1999—), 男, 河北邯郸人, 武汉大学硕士生, 主要研究方向为网络安全。



彭国军 (1979—), 男, 湖北荆州人, 武汉大学教授、博士生导师, 主要研究方向为网络安全、信息系统安全。