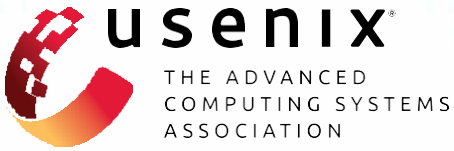

通过活化的ICMP重定向攻击进行路径外网络流量操纵

冯学伟，*清华大学计算机科学与技术系&BNRist*；李琦，*清华大学网络科学与网络空间研究所&BNRist，中关村实验室*；孙坤，*乔治梅森大学信息科学与技术系&CSIS*；钱志云，*加州大学河滨分校*；赵刚，*清华大学计算机科学与技术系&BNRist*；匡晓辉，*北京邮电大学*；傅传璞，*清华大学计算机科学与技术系&BNRist*；徐珂，*清华大学计算机科学与技术系&BNRist，中关村实验室*

https://www.usenix.org/conference/usenixsecurity22/presentation/feng

第31届USENIX安全研讨会论文集的开放访问由USENIX赞助。

通过活化的ICMP重定向攻击进行路径外网络流量操纵

冯学伟[1] , 李琦[2,5] , 孙坤[3] , 钱志云[4] , 赵刚[1] , 匡晓辉[6] 付传普[1] , 徐珂[1,5*]

[1]清华大学计算机科学与技术系&BNRist [2]清华大学网络科学与网络空间研究所&BNRist 3乔治梅森大学信息科学与技术系&CSIS [4]UC河畔分校 中关村实验室 6北京邮电大学

摘要

ICMP重定向是一种机制，它允许终端主机动态地更新其对特定目的地的路由决定。以前的研究表明，ICMP重定向可能被攻击者利用来操纵受害者traf-fic的路由。然而，人们普遍认为，ICMP重定向攻击不是一个现实世界的威胁，因为它们只能在特定的网络拓扑结构（如LAN）下发生。在本文中，我们对ICMP的合法性检查机制进行了系统的研究，发现了检查机制和无状态协议之间的根本差距，导致了广泛的漏洞。特别是，我们发现路径外攻击者可以利用一套无状态协议（如UDP、ICMP、GRE、IPIP和SIT）来轻松制作逃避的ICMP错误信息，从而使ICMP重定向攻击在现实世界中恢复活力，特别是在广域网中造成巨大的破坏。首先，我们表明，路径外攻击者可以通过欺骗互联网上的各种公共服务器，用一个伪造的ICMP重定向消息将其流量误导到黑洞中，从而进行隐蔽的DoS攻击。例如，我们揭示了互联网上有超过43K的流行网站容易受到这种DoS攻击。此外，我们发现互联网上54.47万个开放的DNS解析器和186个Tor节点也是脆弱的。其次，我们表明，通过利用针对NAT网络的ICMP重定向攻击，同一NAT网络中的路径外攻击者可以进行中间人（MITM）攻击，拦截受害者的流量。最后，我们制定了反措施来阻止这些攻击。

1 简介

ICMP重定向机制的设计是为了最大限度地减少特定流量在前往目的地途中必须穿越的路由跳数，从而优化转发路径，减少每个路由器必须处理的流量[18, 67]。一旦确定了一个更好的路由，路由器将发出一个ICMP重定向消息给

*通讯作者：xuke@tsinghua.edu.cn。

告知发端人替代路线。在收到消息并成功验证其合法性后，发端者将更新其路由表，将消息中的网关互联网地址字段设置为其到目的地的新下一跳。几乎所有的主要操作系统都支持ICMP重定向机制。

原则上，ICMP重定向消息应该只由路由器发送，用于报告数据包处理错误[2, 12, 67]。然而，由于目前互联网缺乏对数据包转发路径的验证[42, 87, 88]，任何主机都可以模仿路由器来伪造ICMP错误信息[26]。因此，攻击者可以通过发送伪造的ICMP重定向消息给受害者发起者，将流量从发起者重定向到特定的主机。为了解决这个问题，ICMP规范[6, 12, 31, 67]对发端者收到的ICMP错误信息实施合法性检查机制，即ICMP错误信息应嵌入引发错误信息的原始数据包的至少28个八位字节（即IP头的20个八位字节加上至少前8个八位字节）。

因此，如何逃避ICMP重定向攻击的合法性检查是一个关键问题。在以前的广播网络中，主机由集线器连接，攻击者可以窃听来自发端者的数据，然后将数据嵌入到精心制作的ICMP重定向消息中，以逃避发端者的检查，从而误导发端者的流量[8, 9, 48, 56, 63, 86]。现在，随着交换式网络的广泛部署，主机被交换机或路由器连接起来，路径外攻击者不能再窃听其他主机的网络流量，从而轻易伪造一个可接受的ICMP重定向。因此，以前的ICMP重定向攻击[8, 9, 48, 56, 63, 86]在现代网络拓扑结构中总是失败。

历史上，一些技术博客和讲座已经对路径外攻击者进行恶意ICMP重定向的方法进行了讨论[5, 22, 37, 41, 83]。例如，在内核版本2.6.20之前的Linux系统不检查嵌入UDP数据的ICMP错误信息，因此有可能伪造一个嵌入UDP数据的可接受的ICMP重定向信息，以进行路径外ICMP重定向攻击。然而，现代操作系统会检查嵌入的UDP数据是否存在。

UDP套接字，因此大多数先前的方法将失败[5,22,37,83]。在Kulas的演讲中[41]，ICMP回音信息被利用来伪造重定向信息并逃避发起者的检查机制。然而，建议的ICMP重定向攻击只能在本地网络上成功。此外，在现实世界中，发端者可能出于性能和安全的考虑而禁用ICMP回波[79]，从而挫败了攻击。一般来说，人们普遍认为ICMP重定向攻击不是一个现实世界的威胁，因为它们只可能发生在有限的网络拓扑结构中[8, 9]。

在本文中，我们证明了ICMP重定向攻击可以不受网络拓扑结构的限制，在现实世界中造成严重破坏[8, 9]。特别是，我们发现它实际上在广域网络中广泛适用。我们发现，由于ICMP的合法性检查机制与一系列状态较差的协议（如ICMP、UDP、GRE[25]、IPIP[64]和SIT[61]）之间存在差距，受害者发起人本质上无法检查嵌入这种协议数据的ICMP错误信息的合法性。因此，受害者可能会错误地接受来自路径外攻击者发出的伪造的ICMP重定向消息，从而导致他们的流量被错误地重定向。这个漏洞影响到广泛的主要操作系统，包括Linux 2.6.20及以上版本，FreeBSD 8.2及以上版本，Android 4.3及以上版本，以及Mac OS 10.11及以上版本。[1].

在现代交换网络中，路径外攻击者无法窃听其他主机的流量来制作ICMP重定向消息。然而，我们发现，ICMP的合法性检查机制的模糊性可以被路径外攻击者利用来制作一个逃避的ICMP错误消息。由于无状态协议不能记住先前发送的数据，如果攻击者能迫使受害者发起者弹出无状态协议数据，然后伪造嵌入这种协议数据的ICMP错误消息，那么发起者就很难准确检查消息的合法性。现代操作系统可能会执行一些简单的检查，例如，如果UDP数据被嵌入到收到的ICMP错误信息中，Linux系统自内核2.6.20版本以来会检查相应的UDP套接字的存在。然而，路径外攻击者可以欺骗发端者提前建立一个可预测的UDP套接字，然后他们伪造嵌入了这个已知UDP套接字数据的ICMP错误，受害者发端者执行的检查将很容易被逃避。由于UDP的无记忆性，发端者无法进行进一步的检查，最终会接受伪造的信息。ICMP和无状态协议的合法性检查机制之间的这种内在差距使得路径外攻击者可以轻易地伪造逃避性的ICMP错误。在本文中，我们使用一个伪造的ICMP重定向消息来虚假地更新受害者的路由，然后将其后续流量错误地重定向到

[1] 我们发现，Windows是无懈可击的，因为它没有严格遵守ICMP的规范。Windows默认启用了ICMP重定向机制；然而，它只是放弃了所有收到的ICMP重定向消息，即使这些消息是合法的。

一个指定的主机。

我们证明了我们重新激活的ICMP重定向攻击可以在现实世界中造成严重破坏。首先，一个非路径攻击者可以通过发布一个伪造的ICMP重定向消息，迫使互联网上的一个远程脆弱目标将其流量路由到黑洞（默认情况下主机转发功能被禁用），从而导致一个隐蔽的DoS攻击。我们的实验表明，互联网上有超过43,000个流行的网站是脆弱的。此外，我们证明我们的DoS攻击甚至可以在切断发起者和目的地之间的通信时，关闭DNS和Tor等后端服务的整个操作，从而导致更广泛的影响。我们发现，互联网上54,470个开放的DNS解析器和186个Tor节点容易受到我们的攻击。其次，当攻击者和受害者重新在同一网络中时，我们表明路径外攻击者可以演变成中间人（MITM），然后进行各种劫持攻击，例如，在NAT（网络地址转换）[81]网络中劫持DNS请求。

最后，我们制定了不同的反击措施来对付这些攻击，并系统地衡量其有效性。首先，我们建议改变网络设置以阻止互联网上的欺骗性ICMP重定向消息，这可以防止在ISP部署过滤机制的情况下发生的再移动DoS攻击。其次，我们评估了采用协议变化的可能性，以改善ICMP消息的合法性检查机制，例如，在UDP中嵌入秘密以验证通信。最后，我们建议严格区分无状态协议和有状态协议，在无状态协议上禁用ICMP重定向机制。这一对策可以有效地击败上述DoS攻击和MITM攻击。此外，该对策可以很容易地部署，因为它只需要在担心ICMP重定向攻击的特定主机上进行修改。我们实现了一个原型，并在我们的真实世界网络中评估了这个对策。实验结果表明，它可以有效地防止攻击，而对网络性能的副作用很小。

贡献。我们的主要贡献有以下几点：

- 我们发现了ICMP和无状态协议的合法性检查机制之间的一个基本差距，我们揭示了这个差距可能导致广泛的主要操作系统的漏洞，包括Linux 2.6.20及以后，FreeBSD 8.2及以后，Android 4.3及以后，Mac OS 10.11及以后。
- 我们证明ICMP重定向攻击可以在互联网上形成，从而在现实世界中造成严重破坏。我们发现互联网上有超过43,000个流行网站、54,470个开放的DNS解析器和186个Tor中继节点容易受到我们的攻击。
- 我们分析了其根本原因，并提出了一个增强的ICMP合法性检查机制来防止攻击。一个原型验证了我们对策的有效性。

道德方面的考虑。在本文中，我们进行了两种类型的真实世界实验，以验证所确定的攻击的可行性和影响，即发现互联网上易受DoS攻击的公共服务器（见第5节）和劫持我们校园网络中易受攻击的DNS转发器的请求（见第6节）。在进行实验时，我们把伦理道德作为首要任务。

在发现互联网上易受攻击的公共服务器的实验中，我们使用我们自己的测试平台的机器作为公共服务器的目的地。通过发布精心制作的ICMP重定向，我们只改变了服务器数据包对我们自己机器的路由，因此我们的实验不会影响正常用户对服务器的访问。此外，一个ICMP重定向消息对服务器产生的负载可以忽略不计。实验结束后，我们通过发布一个补救性的ICMP重定向消息（即指定服务器的默认网关为到我们机器的下一跳）来恢复服务器的路由变化。我们还确认了治疗性ICMP重定向消息的有效性。

在我们的校园网进行劫持DNS的实验之前，我们向网络管理员解释了我们攻击的细节和潜在的风险。我们获得了他们的批准，只为研究目的进行实验。在管理员的帮助下，我们在午夜进行实验。管理员确定在我们进行实验之前没有用户访问目标网络，防止我们的实验对正常用户产生潜在的隐私风险。此外，为了尽量减少对转发者的DNS缓存的影响，我们只拦截转发者对一个特定网站（即我们实验中的目标网站 "www.yahoo.com"）的DNS查询。一旦实验结束，网络管理员将DNS转发器重置为正常状态。

2 背景介绍

2.1 网络流量的ICMP重定向

自1981年以来，作为RFC 792的标准[67]，ICMP重定向机制被路由器用来通知发端者从发端者到目的地的更优化路径。它减少了到达目的地所必须经过的跳数。图1显示了ICMP重定向的基本程序。当发端人的网关收到一个IP数据包时，该网关将检查其路由表以确定下一个网关的地址。如果下一个网关和由数据包的源IP地址确定的发端者在同一个网络上，则一个ICMP重定向消息将从网关发送给发端者。生成的ICMP重定向消息建议发端者将其目的地网络的traf-fic直接发送到下一个网关，而不是当前的网关，因为直接通过下一个网关转发是通往目的地的较短路径。

一旦发端人收到ICMP重定向消息

并且该报文通过其检查，发端者将下一个网关设置为其到目的地的路线的下一跳。在ICMP规范[67]中，ICMP重定向消息的Type字段被指定为5，Code字段可以指定为0、1、2和3，分别表示为网络重定向数据包、为主机重定向数据包、为服务类型和网络重定向数据包、为服务类型和主机重定向数据包。下一个网关是在ICMP重定向消息的网关互联网地址字段中指定的。

ICMP重定向机制对于减少路由跳数和实现路由器之间的负载平衡非常有用。如果重定向机制被禁用，发端者将不知道到目的地的最优化路由。因此，ICMP重定向机制在广泛的主要操作系统的IP实现中是默认启用的，例如，Linux 2.6.20及以后，FreeBSD 8.2及以后。配备这些操作系统的发起人默认接受ICMP重定向消息，一旦消息通过检查机制，就将其流量重定向到指定的网关互联网地址（即，下一个网关）。

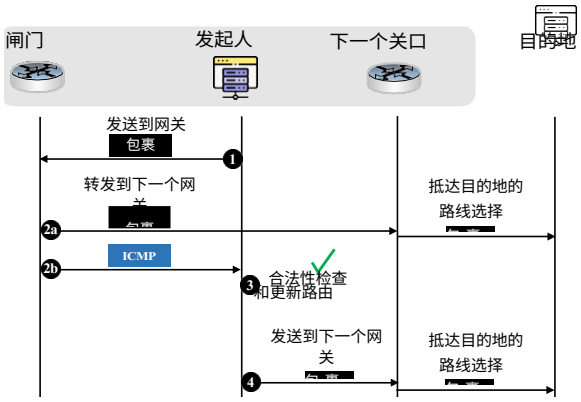

图1：通过ICMP 重定向优化路由路径。

2.2 对ICMP错误的合法性检查

ICMP重定向机制也可能被攻击者利用来操纵网络流量。攻击者可以向发起者发送一个伪造的ICMP重定向消息，这表明所有未来的目的地流量必须被重定向到一个特定的系统，作为目的地的较短路径。

为了防止ICMP重定向的滥用，当收到ICMP重定向消息时，发起人会进行两次检查[6, 12, 67]。首先，发端者检查该消息是否由其默认网关发送，即ICMP重定向消息的源IP地址应被指定为默认网关的IP地址。第二，ICMP错误信息应该携带触发错误信息的原始数据包的至少28个字节（即IP头的20个字节加上至少前8个字节）。这28个八位字节的数据将被发端者用来将信息与相关的数据相匹配。