DeepL
订阅DeepL Pro以翻译大型文件。
欲了解更多信息，请访问www.DeepL.com/pro。

响应的过程，并检查消息的合法性。此外，根据较新的标准RFC 1812 [6]，ICMP错误消息应携带触发数据包的大部分内容，但不超过576个八位字节。

2. 3对检查的现有规避

不幸的是，即使实现了对ICMP重定向的合法性检查，攻击者仍然可能逃避检查，进行ICMP重定向攻击。由于互联网上的IP地址欺骗的脆弱性，第一个检查很容易被规避。非路径攻击者可以冒充受害者发起者的网关，发出欺骗性的ICMP重定向消息。根据先前的研究[44, 49]，互联网上约有四分之一的自治系统（AS）没有过滤离开其网络的带有欺骗性源IP地址的数据包。在本文中，我们发现互联网上有超过5100个AS没有执行有效的入口过滤[7, 28]。因此，这些AS中的网关带有欺骗性源IP地址的ICMP重定向消息可以通过整个路由路径并被转发到受害者的发端（详见后面的第4节）。

对ICMP重定向消息中嵌入的有效载荷的第二次检查对于路径外的攻击者来说更难逃避，即使发起者只执行RFC792中定义的较弱的检查机制（即检查原始数据包的前28个八位字节）。如图2所示，当发端者使用TCP作为高级协议与他人进行通信时，攻击者必须猜测识别TCP连接的四元组和发端者发送窗口中的序列号来制作一个规避的ICMP重定向消息。特别是，路径外的攻击者很难猜到这些值，因为源端口和序列号是随机产生的。[2]在现代操作系统中[32]。

图2：嵌入TCP的ICMP重定向 消息。

在本文中，我们表明，无论检查的是28个八位数还是576个八位数，都可以顺便通过第二次检查。这是由于ICMP的合法性检查机制和无状态协议之间的差距，这最终导致了接下来描述的现实世界的ICMP重定向攻击。

[2] 初始序列号是随机产生的，随后的序列号在其基础上单调递增。

3 检查ICMP错误的漏洞

3.1 ICMP合法性检查中的漏洞

与TCP不同，无状态协议不能记住先前发送的数据。因此，如果路径外的攻击者伪造了嵌入这种协议数据的ICMP错误信息，发端者就很难准确地检查嵌入数据的合法性。因此，受害者可能会接受这些伪造的信息。一旦伪造的ICMP重定向消息被接受，受害者将根据消息中指定的新网关虚假地更新其路由。因此，由IP承担的整个流量将受到影响并被交叉攻击。在实践中，当受害者找到一个更好的下一跳时，重定向所有后续的流量是合理的，因为流量路由发生在IP层，与上层协议无关。然而，不同协议之间相互作用的复杂性给目前的网络原则带来了许多挑战[26]。

目前的ICMP实现可能对收到的嵌入无状态协议数据的ICMP错误消息进行一些检查。例如，当收到嵌入UDP数据报的消息时，Linux内核2.6.20及以后的版本会检查它和目的地之间是否存在UDP套接字。这种检查可以防止以前的ICMP重定向攻击[22, 37, 83]。然而，我们发现，由于ICMP的合法性检查机制存在固有的缺陷，这种检查很容易被规避。

在实践中，现代操作系统为轻量级服务（如NTP、SNMP、DHCP、DNS和TFTP）默认开放了几个公开的UDP端口。[3]因此，攻击者可以首先探测受害者的这种开放的UDP端口，然后欺骗受害者在探测的开放端口上为远程目的地生成一个可预测的UDP套接字。之后，攻击者伪造一个ICMP重定向消息给受害者，其中嵌入了已知的UDP套接字和一些任意的填充数据。由于UDP的无状态性，填充数据不能被准确检查。因此，伪造的ICMP重定向消息将逃避安全检查并被错误地接受，即成功地对受害者进行非路径ICMP重定向攻击。除了UDP，我们发现ICMP、GRE[25]、IPIP[64]和SIT[61]的无状态协议也可以被路径外攻击者利用来逃避ICMP的合法性检查机制。在我们的攻击中，我们以UDP为例来阐述和利用这个漏洞。请注意，使用无状态协议来触发ICMP合法性检查机制的漏洞的方法是通用的。路外攻击者可以利用无状态协议来伪造所有类型的ICMP错误信息（不仅仅是ICMP重定向信息）来逃避检查。

[3] 一个开放的端口足以进行我们的攻击。例如，在Linux内核版本的Ubuntu 20.04中，超过6个UDP端口是默认开放的。5.4.我们发现互联网上有超过43K个网络服务器、54K个开放的DNS解析器和186个Tor中继节点至少开放了一个UDP端口（见§5）。

3.2 易受影响的实施

所发现的差距影响了广泛的实现，即Linux 2.6.20（2007年2月发布）及以后，FreeBSD 8.2（2011年2月发布）及以后，An- droid 4.3（2012年6月发布）及以后，Mac OS 10.11 （2015 年9 月发布）及以后。在Linux 系统、FreeBSD系统、内核版本6.0之前的Android系统和内核版本10.11.6之前的Mac OS中，ICMP重定向机制被默认启用。在安卓系统中，一旦内核中启用了ICMP重定向机制，普通用户很难手动禁用该机制，因为禁用的操作需要root权限[1]，而世界上只有大约7.6%的安卓系统用户对他们的设备进行了root[3]。对于内核版本10.11.6之后的Mac OSs，一旦ICMP重定向机制通过*sysctl*的参数被启用，Mac OSs也会变得脆弱。

我们还审查了Linux系统和FreeBSD系统的源代码，以确认它们对我们的攻击确实是脆弱的。例如，图3显示了自Linux内核2.6.20版本以来处理嵌入UDP数据报的ICMP错误信息的代码。[4].可以看出，Linux会首先检查套接字的存在（在第106行）。由于UDP的无状态和无记忆性，Linux不能对嵌入的UDP数据进行进一步的检查（不像TCP会进一步检查以确认携带的序列号是否在其发送窗口内）。因此，只要到远程目的地的套接字存在，Linux就会为目的地重定向出站流量（在第113行）。然而，正如我们之前在第3.1节所描述的，攻击者可以很容易地制作一个UDP套接字来逃避这种检查，从而欺骗受害者顺从地重定向其流量。

```
100  空白 u d p 4 _ lib_ e r r ( )
101  {
102      .....
103      const int type = icmp_hdr(skb)->type;
104      const int code = icmp_hdr(skb)->code;
105      struct sock *sk;
106      sk = u d p 4 _ lib_ l o o k u p ( );
107      if (!sk) {
108                  ICMP_INC_STATS(net, ICMP_MIB_INERRORS)
                    ;
109              return; /* 没有套接字的错误 */
110      }
111      switch (type) {
112              case ICMP_REDIRECT:
113                      ipv4_sk_redirect( );
114      }
115      .....
116  }
```

图3：处理嵌入UDP的ICMP错误。

3.3 炮制回避的ICMP重定向

图4说明了嵌入已知UDP数据报的伪造的ICMP 重定向消息的结构，它可以

[4] Linux自内核4.20.17版本以来引入了一些小的变化，但基本逻辑没有改变。

被用来规避ICMP规范中的检查机制。在IP头中，协议文件被指定为ICMP，源IP地址和目的IP地址分别被指定为网关的IP地址和受害者发起人的IP地址。然后在ICMP头中，类型字段被指定为5，表示这是一个ICMP重定向消息。代码字段的值不是唯一的，攻击者可以选择四个值中的任何一个（即0、1、2或3）来重定向受害者发端者的网络流量，用于下一个嵌入UDP数据报中指定的目的地。网关互联网地址字段指定了发端人在前往目的地途中的新网关。

无论RFC792和RFC1812中定义的检查是否被实施，我们伪造的ICMP重定向信息都能发挥作用，因为检查机制在设计上对无状态协议（即我们演示的UDP）是无效的。此外，我们发现RFC 1812（即尽可能多地检查触发数据包，但不超过576个字节）在我们在§3.2中列出的易受攻击的操作系统中没有严格实施。因此，在实践中，攻击者只需要制作图4中UDP数据报的前28个八位字节的数据，以逃避检查机制，然后成功执行我们的攻击。

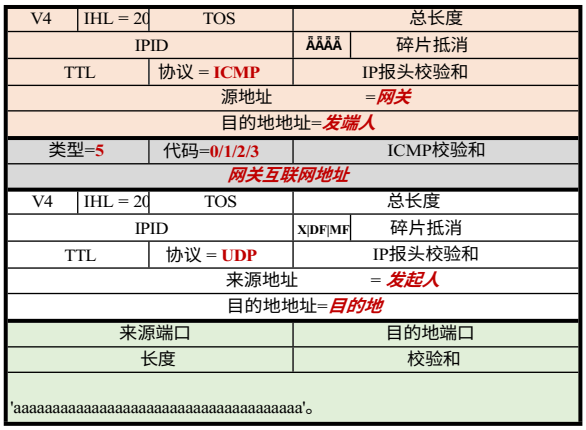


图4：伪造的ICMP ，嵌入UDP的重定向。

通过制作这样一个回避的ICMP重定向消息，攻击者可以操纵受害者的流量来构建非路径攻击，即（i）当攻击者不与服务器居住在同一网络中时，对互联网上的脆弱服务器进行隐蔽的远程DoS攻击，或者（ii）如果攻击者是一个与受害者居住在同一网络中的正常用户，则劫持受害者的流量来构建MITM攻击。

4 伪造互联网上的ICMP重定向

我们的远程DoS攻击的一个必要条件是，由路径外攻击者制作的恶意ICMP重定向消息可以转发给远程受害者。在本节中，我们将进行

表1：在互联网上转发ICMP重定向信息。

AS交叉 / 寄件人	接收器	亚洲 北京 159.226.*.202	东京 124.156.*.135	孟买 119.28.*.146	新加坡 150.109.*.233	香港 43.129.*.233	美国 加利福尼亚州 170.106.*.100	多伦多 49.51.*.40	弗吉尼亚州 170.106.*.40	欧洲 法兰克福 162.62.*.44	莫斯科 162.62.*.197
美国	加州 47.88.*.24	AS7497 AS174 AS2914	AS2914	AS6453	AS7473 AS4766	AS6453 AS9304	AS8003	AS3356 AS2914	AS2914 AS3356	AS1299 AS2914	AS6762 AS2914 AS31133
	弗吉尼亚州 47.90.*.227	AS7497 AS174	AS2516 AS3356	AS174 AS9498	AS6453 AS3356	AS3491 AS174	AS3356	AS3356	AS32098	AS3356	AS3356
欧洲	伦敦 8.208.*.114	AS7497 AS174 AS3356 AS45102	AS2516 AS3356 AS45102	AS9498 AS45102	AS7473 AS1299 AS45102	AS6453 AS3491 AS3356 AS45102	AS3356 AS45102	AS3356 AS45102	AS3356 AS45102	AS1299 AS45102	AS6939 AS209141 AS45102
澳大利亚	悉尼 47.74.*.68	AS7497 AS7474 AS3491 AS45102 AS7473	AS2914 AS7474 AS7473 AS45102	AS7473 AS7474 AS9498 AS45102	AS7473 AS7474 AS45102	AS7474 AS7473 AS45102 AS9304	AS6453 AS7474 AS7473 AS45102	AS6453 AS7474 AS45102 AS7473	AS7474 AS6461 AS45102 AS7473	AS1299 AS7474 AS45102 AS7473	AS6939 AS45102 AS15412 AS209141
亚洲	雅加达 147.139.*.126	AS7497 AS3491 AS10217 AS2914	AS2914 AS10217	AS7473 AS9498 AS135391	AS135391	As3491 As10217 As2914	AS6453 AS2914 AS10217	AS6453 AS2914 AS10217	AS3356 AS10217 AS2914	AS1299 AS3356 AS10217 AS2914	AS2914 AS10217 AS3356
	青岛 118.190.*.74	AS7497 AS37963	AS4837 AS45102 AS2914	AS4837 AS37963 AS6453 AS4755	AS7473 AS58541 AS45102 AS4134 AS4809	AS37963 AS58541 AS4134 AS4809	AS4134 AS45102 AS58541	AS6453 AS4837 AS45102	AS7018 AS4837 AS37963	AS4837 AS1299 AS37963 AS45102	AS4837 AS12389 AS45102
	迪拜 47.91.*.206	As3491 As6762 As45102 AS15802	AS2914 AS45102 AS15802	AS45102 AS9498	AS8003	AS9304 AS45102 AS15802	AS3356	AS3356 AS45102	AS3356 AS45102 AS15802	AS45102	AS31133 AS45102
	北京 183.173.*.12	AS7497	AS2914 AS4134	AS4637 AS9498	AS4134 AS4809	AS4134 AS4809	AS4134	AS6453 AS4637	AS4134 AS3356	AS4134 AS3356	AS4134 AS31133
	吉隆坡 47.250.*.16	AS7497 AS3491 AS2914	AS2914	AS9930 AS9498	AS9930	AS3491 AS2914	AS6453 AS2914	AS6453 AS2914	AS2914 AS3356	AS2914 AS3356	AS2914 AS3356

对向远程受害者发送精心制作的ICMP重定向消息的可行性进行测量研究。

4.1 在互联网上转发重定向

根据ICMP规范[12, 67]，ICMP重定向消息应该只由当前第一跳门路向所连接的主机发出，这意味着ICMP重定向消息不应该在网际网络上被转发。因此，如果ICMP重定向信息出现在互联网上，它们应该被过滤机制[7, 28, 39]默默地丢弃，只允许合法流量通过网络。然而，通过对互联网的广泛测量研究，我们发现，精心制作的ICMP重定向消息仍然被允许穿越相当数量的AS，从而在互联网上成功转发。

实验设置。我们在全球4个地点部署了19个有利位置，以测试在互联网上不同AS中转发精心制作的ICMP重定向消息的可行性。我们从其中9个有利位置制作ICMP重定向，然后将制作好的消息发送到其余10个位置（关于我们均匀分布在世界各地的有利位置的更多细节，见表1）。请注意，我们在这个实验中没有进行任何IP欺骗，因为我们的目标是看重定向信息本身是否能在互联网上成功转发。

实验结果。表1显示了我们的实验结果。我们发现，在我们的90次测量中，精心制作的信息总是可以被转发到接收器，而没有任何

在互联网上的限制，即使信息的转发跨越了几个AS，而且信息的指定源IP地址显然是非法的，即信息的源IP地址是根本不可能是接收方的网关的发件人。

4.2 在目标AS中接收欺骗的重定向信息

除了在网间转发ICMP重定向消息，我们的远程DoS攻击还要求受害者发起人所在的目标AS不会丢弃伪造的ICMP重定向消息，该消息的源IP地址是AS内受害者的网关。

在我们对互联网的实证研究中，我们发现大量易受攻击的AS允许被欺骗的ICMP重定向信息（其源IP地址为这些AS内的网关）进入。这些被欺骗的信息将被成功地转发到附属于网关的受害者发起者，从而操纵受害者的网络流量（关于受害者发起者和互联网上相应的脆弱AS的检测细节，见第5.2节）。

我们完全检测到5184个脆弱的目标AS（位于全球185个国家）没有过滤欺骗的ICMP重定向消息。考虑到互联网上大约四分之一的AS还没有实施有效的过滤机制来阻止欺骗的数据包，这并不奇怪[44, 49]。表2列出了30个脆弱AS的详细信息。例如，如第一行所示，一个IP地址为154.54.x.157的网关位于AS 174，它位于美国，属于Cogent公司。

通信。我们用这个网关的欺骗性源IP地址伪造一个ICMP重定向消息，并将该消息发送到连接到这个网关的受害者（我们在Alexa前100万个网站列表中检测到的一个脆弱的网络服务器，更多细节见§5.3）。最后，被欺骗的ICMP重定向消息被成功地转发给受害者。

表2：允许欺骗性重定向信息的易受攻击的AS。

帐户号：	GatewayAS No.	组织机构	地点
154.54.x.157		AS174Cogent Comm.	美国
64.86.x.66	AS6453	TATA Comm. (AMERICA)	美国
45.79.x.5	AS63949	Linode, LLC	美国
204.93.x.159	AS23352	服务器中央网络	美国
72.29.x.133	AS7393	CYBERCON, INC.	美国
148.163.x.24	AS53755	输入输出洪流有限责任公司	美国
64.74.x.198	AS63410	私人系统网络	美国
209.58.x.15	AS394380	美国租赁网	美国
188.170.x.58	AS31133	PJSC MegaFon	RU
92.53.x.34	AS49505	OOO网络	RU
109.234.x.250	AS50340	OOO网络	RU
62.67.x.186	AS3356	Level3, LLC	AAA
213.239.x.230	AS24940	Hetzner Online GmbH	ÄÄÄ
198.27.x.92	AS16276	OVH SAS	共和
89.30.x.146	AS31216	BSOCOM	共和
185.17.x.66	AS42831	英国专用服务器	GB
87.245.x.221	AS9002	RETN有限公司	GB
125.22.x.166	AS9498	BHARTI Airtel	纳入
183.83.x.29	AS18209	阿特里亚聚合	纳入
218.145.x.26	AS4766	韩国电信	KR
58.159.x.178	AS17506	ARTERIA网络	蒋介
159.226.x.203	AS7497	计算机网络	氯化
195.142.x.162	AS34984	TELCOM iletisim	ÄAA
80.67.x.207	AS42708	GleSYS AB	ÄÄÄ
83.137.x.204	AS47692	Nessus GmbH	淘宝
103.245.x.150	AS17660	DrukNet ISP	英国
103.252.x.129	AS45638	协同批发	AU
118.98.x.254	AS18051	普斯泰科姆	身份
113.21.x.217	AS38082	真正的互联网	钍
45.138.x.1	AS207640	专家解决方案	创业

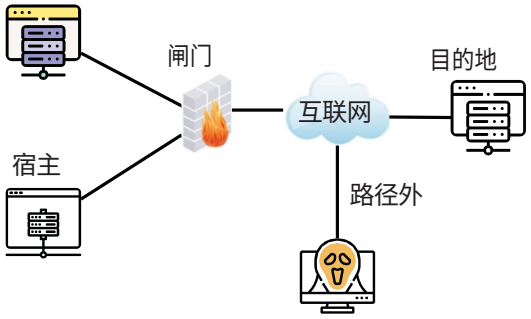
5 隐蔽的远程DoS攻击

在这一节中，我们提出了一种隐蔽的DoS攻击，它可以远程启动，利用弱的ICMP合法性检查机制，切断一对IP地址之间的通信。它不仅可以针对个人用户，例如，阻止一个人访问一个网站，还可以针对服务器之间的通信，例如，关闭DNS解析器与特定的权威名称服务器联系以解析某些域名。当Tor节点之间的通信被切断时，甚至有可能关闭整个服务的运作，如Tor。我们首先介绍了威胁模型和我们攻击的设计。然后，我们进行实证研究，以确定互联网上脆弱的公共服务器。我们发现43,081个流行的网站，54,470个开放的DNS解析器和186个居住在5,184个AS和185个国家的Tor中继节点都容易受到我们的DoS攻击。

5.1 威胁模型

图5说明了我们的路径外DoS的威胁模型。该模型由四个主机组成：1）一个受害者发起者（在不同的攻击方案中，受害者发起者可能是一个网络服务器，一个开放的DNS解析器或一个Tor中继节点），2）一个与受害者发起者连接到同一网关的邻近主机，3）一个受害者目的地（相应地，在不同的攻击方案中，受害者目的地可能是一个网络客户端，一个权威的名称服务器或一个下一跳的Tor重铺节点），4）一个非路径攻击者。路外攻击者的目的是假装成网关，并伪造一个ICMP重定向消息给发端者，从而将发端者对目的地的网络流量恶意地重定向到邻近的主机。由于主机在默认情况下是转发失效的，它们将作为黑洞，丢弃发端者的流量，这意味着路径外攻击者对受害发端者进行了成功的DoS攻击。为了完成DoS攻击，需要满足以下要求。

受害者的始作俑者



攻击者

图5：DoS攻击的威胁模型。

可追踪的网关。网关的IP地址对攻击者来说是已知的，因为攻击者需要冒充网关来制作ICMP重定向消息。一旦发端者的IP地址被确定，其网关的IP地址就可以通过traceroute[46]观察到。

IP欺骗。路外攻击者有能力发送带有网关IP地址的欺骗性数据包。先前的研究表明，互联网上大约四分之一的AS没有过滤离开其网络的带有欺骗源地址的数据包[44, 49]，从防弹托管节点租借这样的机器是很容易的[50]。此外，最近的一项研究[20]发现，互联网上有69.8%的AS不执行入口过滤来阻止欺骗的数据包，这进一步证明了IP欺骗的严重性。

脆弱的目标。目的地的出站流量将被误导的受害发起人必须配备§3.2中列出的易受攻击的操作系统。因此，精心制作的ICMP重定向消息可以逃避发端者的检查，使发端者的路由中毒。

活的邻居主机。在目前的ICMP实现中，发端者将检查主机的可用性，当它