分布式拒绝服务攻击与防范

专业：网络12-1-35
姓名：杨兴杰
2015.10.5

1 分布式拒绝服务的由来及原理

1.1 分布式拒绝服务的起源

分布式拒绝服务 用户对于这个话题似乎已经不再陌生,在当今的网络当中用户能够经常听见此类事件的发生，比如说唐山黑客事件中，所利用的黑客技术就是DDOS攻击。这种攻击方法的可怕之处是会造成用户无法对外进行提供服务，时间一长将会影响到网络流量，造成用户经济上的严重损失。造成这种类型攻击的最主要原因就是商业竞争、打击报复和网络敲诈等多种因素，从实际情况来说DDOS是不可能完全防范的，不过用户必须要从最大程度上做好防范DDOS攻击的措施，使用户在遭受DDOS攻击后的损失减至最低。英文名DDOS，是Distributed Denial of Service的缩写,俗称洪水攻击。

分布式拒绝服务的起源：

1999年7月份左右，微软公司的视窗操作系统的一个bug被人发现和利用，并且进行了多次攻击，这种新的攻击方式被称为“分布式拒绝服务攻击”即为“DDos（Distributed Denial Of Service Attacks）”。这也是一种特殊形式的拒绝服务攻击。单一的DoS攻击一般是采用一对一方式的，当攻击目标CPU速度低、内存小或者网络带宽小等等各项性能指标不高它的效果是明显的。随着计算机与网络技术的发展，计算机的处理能力迅速增长，内存大大增加，同时也出现了千兆级别的网络，这使得DoS攻击的困难程度加大了 - 目标对恶意攻击包的"消化能力"加强了不少，例如你的攻击软件每秒钟可以发送3,000个攻击包，但我的主机与网络带宽每秒钟可以处理10,000个攻击包，这样一来攻击就不会产生什么效果。这时候分布式的拒绝服务攻击手段（DDoS）就应运而生了

DDOS的攻击策略侧重于通过很多“僵尸主机”(被攻击者入侵过或可间接利用的主机)向受害主机发送大量看似合法的网络包，从而造成网络阻塞或服务器资源耗尽而导致拒绝服务，分布式拒绝服务攻击一旦被实施，攻击网络包就会犹如洪水般涌向受害主机，从而把合法用户的网络包淹没，导致合法用户无法正常访问服务器的网络资源。

1.2 分析分布式拒绝服务攻击的原理

- DoS(拒绝服务)的英文全称是Denial of Service，它的目的就是拒绝你的服务访问，破坏组织的正常运行，最终会使你的部分Internet连接和网络系统失效。DoS的攻击方式是资源的，利用合理的服务请求来占用过多的服务资源，从而使合法用户无法得到服务的响应以及电子商务的兴起。随着网络的攻击发展成为一种隐蔽性强、破坏性大的攻击手段。拒绝服务攻击分类：

常见的DoS 攻击类型有四种：

一 带宽消耗 攻击者攻击多带宽点集中拥塞受害者的网络连接。

二 资源衰竭攻击 攻击者消耗掉某个网络的所有可用带宽或征用内存之类的系统资源，但滥用其消耗额外的系统资源。

三 编程缺陷 是指应用程序或者操作系统在处理异常条件时的失败。每个程序、操作系统都有缺陷，这个规律，向目标系统发送非陷异常正，常攻击者利用。常格式的分组让网络协议栈或系统都陷入异常格式的失败。

四 路由和DNS攻击 操纵路由表项（利用路由协议认证机制的弱点，变换合法路径）；改变受害者DNS高速缓存的正确地址信息。

拒绝服务攻击的进一步发展——分布式DOS攻击，是一种基于DoS的特殊形式的拒绝服务攻击，是一种分布、协作的大规模攻击方式，主要瞄准比较大的站点，像商业公司、搜索引擎和政府部门的站点。DDoS攻击是利用一批受控制的机器向某一台机器发起攻击，攻击者实用的计算机数量和能占用的带宽是没有限制的，因此具有极大的破坏性。

凡是能导致合法用户不能够访问正常网络服务的行为都算是拒绝服务攻击。也就是说拒绝服务攻击的目的非常明确，就是要阻止合法用户对正常网络资源的访问，从而达成攻击者不可告人的目的。

虽然同样是拒绝服务攻击，但是DDOS和DOS还是有所不同，DDOS的攻击策略侧重于通过很多“僵尸主机”（被攻击者入侵过或可间接利用的主机）向受害主机发送大量看似合法的网络包，从而造成网络阻塞或服务器资源耗尽而导致拒绝服务，分布式拒绝服务攻击一旦被实施，攻击网络包就会犹如洪水般涌向受害主机，从而把合法用户的网络包淹没，导致合法用户无法正常访问服务器的网络资源，因此，拒绝服务攻击又被称之为“洪水式攻击”，常见的DDOS攻击手段有SYN Flood、ACK Flood、UDP Flood、ICMP Flood、TCP Flood、Connections Flood、Script Flood、Proxy Flood等；而DOS则侧重于通过对主机特定漏洞的利用攻击导致网络栈失效、系统崩溃、主机死机而无法提供正常的网络服务功能，从而造成拒绝服务，常见的DOS攻击手段有TearDrop、Land、Jolt、IGMP Nuker、Boink、Smurf、Bonk、OOB等。如果说计算机与网络的处理能力加大了10倍，用一台攻击机来攻击不再能起作用的话，攻击者使用10台攻击机同时攻击呢？用100台呢？DDoS就是利用更多的傀儡机来发起进攻，以比从前更大的规模来进攻受害者

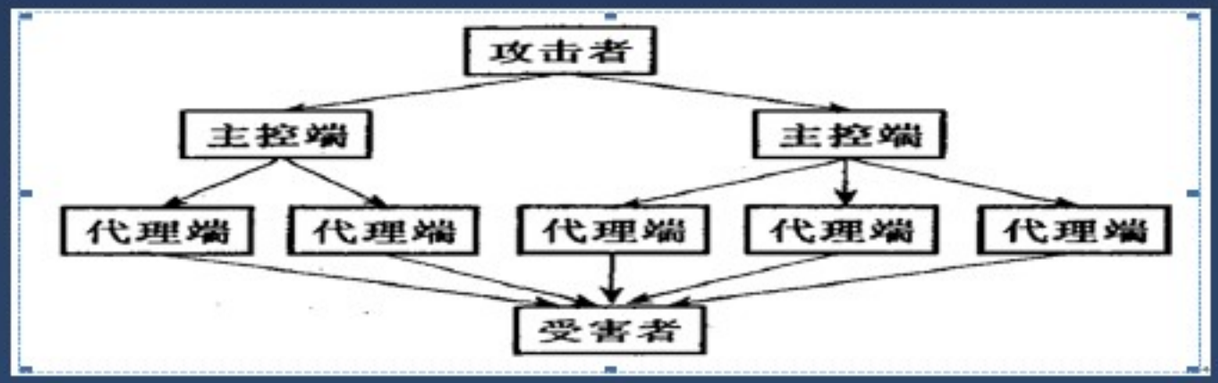

图1.2分布式拒绝服务攻击原理

从图中可以看出，DDoS的攻击分为三层:攻击者、主控端和代理端，三者在攻击中扮演着不同的角色。攻击者 攻击者所用的计算机是攻击主控台。攻击者操纵整个攻击过程，并向主控端发送攻击命令。主控端 主控端是攻击者非法侵入并控制的一些主机，这些主机还分别控制着大量的代理主机。主控端主机的上面安装了特定的程序，因此它们可以接受攻击者发来的特殊指令，并且可以把这些命令发送到代理主机上。设置主控端的目的是隔离网络联系，保护攻击者在攻击时不受监控系统的跟踪，同时能更好的协调进攻。

代理端 代理端同样是攻击者侵入并控制的一批主机，在它们的上面运行攻击器程序，接受和运行主控端发来的命令。代理端主机是攻击的直接执行者。

攻击者发起DDoS攻击的第一步就是在Internet上寻找有漏洞的主机，进入系统后在其上面安装后门程序，获得对系统的直接访问权。第二步是在入侵主机上安装攻击程序，让一部分主机充当攻击的主控端，另一部分主机充当攻击的代理端，最后在攻击者的调遣下对攻击对象发起攻击。

由于攻击者的位置灵活，又使用了常见的协议，因此在攻击时不会受到监控系统的跟踪，身份也不易被发现。

高速广泛连接的网络给大家带来了方便，也为DDoS攻击创造了极为有利的条件。在低速网络时代时，黑客占领攻击用的傀儡机时，总是会优先考虑离目标网络距离近的机器，因为经过路由器的跳数少，效果好。而现在电信骨干节点之间的连接都是以G为级别的，大城市之间更可以达到2.5G的连接，这使得攻击可以从更远的地方或者其他城市发起，攻击者的傀儡机位置可以在分布在更大的范围，选择起来更灵活了。

2.1DOS以及DDOS的攻击方法

对DoS而言，其攻击方式很多，主要使用的攻击有3种，分别是TCP-SYN flood、UDP flood和ICMP flood。当用户进行一次标准的TCP连接时，会有一个3次握手过程。首先是请求服务方发送一个SYN消息，服务方收到SYN后，会向请求方回送一个SYN-ACK表示确认，当请求方收到SYN-ACK后，再次向服务方发送一个ACK消息，这样，一次TCP连接建立成功。但是TCP-SYN flood在实现过程中只进行前2个步骤：当服务方收到请求方的SYN-ACK确认消息后，请求方由于采用源地址欺骗等手段使得服务方收不到ACK回应，于是，服务方会在一定时间处于等待接收请求方ACK消息的状态。对于某台服务器来说，可用的TCP连接是有限的，如果恶意攻击方快速连续地发送此类连接请求，该服务器可用的TCP连接队列将很快被阻塞，系统可用资源急剧减少，网络可用带宽迅速缩小，长此下去，网络将无法向用户提供正常的服务。由于UDP（用户数据包协议）在网络中的应用比较广泛，基于UDP攻击种类也较多。如今在Internet上提供WWW和Mail等服务设备通常是使用 Unix的服务器，它们默认一些被恶意利用的UDP服务，如echo和chargen服务，它会显示接收到的每一个数据包，而原本作为测试功能的 chargen服务会在收到每一个数据包时随机反馈一些字符，如果恶意攻击者将这2个UDP服务互指，则网络可用带宽将很快耗尽

目前，我们知道的对网络进行DDoS攻击所使用的工具有：Trinoo、Tribe Flood Network(TFN)、TFN2k和Stacheldraht等。它们的攻击思路基本相近。

1．Trinoo：它是基于UDP flood的攻击软件，它向被攻击目标主机的随机端口发出全零的4字节UDP包，在处理这些超出其处理能力垃圾数据包的过程中，被攻击主机的网络性能不断下降，直到不能进行使用。此攻击方法用得不多。

2．TFN：它是利用ICMP给代理服务器下命令，其来源可以做假。它可以发动SYN flood、UDP flood、ICMP flood及Smurf（利用多台服务器发出海量数据包，实施DoS攻击）等攻击。TFN的升级版TFN2k的特点是：对命令数据包加密、更难查询命令内容、命令来源可以做假，还有一个后门控制代理服务器

3．Stacheldraht：对命令来源做假，而且可以防范一些路由器用RFC2267过滤。若检查出有过滤现象，它将只做假IP地址最后8位，从而让用户无法了解到底是哪几个网段的哪台机器被攻击。此外，它还具有自动更新功能，可随软件的更新而自动更新。

像Trinoo和TFN等攻击软件都是可以从网上随意找到的公开软件，所以任何一个上网者都可能构成网络安全的潜在威胁。

2.2 被DDOS攻击时的现象

1.被攻击主机上有大量等待的TCP连接

2.网络中充斥着大量的无用的数据包，源地址为假

3.制造高流量无用数据，造成网络拥塞，使受害主机无法正常和外界通讯

4.利用受害主机提供的服务或传输协议上的缺陷，反复高速的发出特定的服务请求，使受害主机无法及时处理所有正常请求

5. .系统服务器CPU利用率极高，处理速度缓慢，甚至宕机

6. 被DDoS攻击后，服务器出现木马、溢出等异常现象

当对一个Web站点执行 DDoS 攻击时，这个站点的一个或多个Web服务会接到非常多的请求，最终使它无法再正常使用。在一个DDoS攻击期间，如果有一个不知情的用户发出了正常的页面请求，这个请求会完全失败，或者是页面下载速度变得极其缓慢，看起来就是站点无法使用。典型的DDoS攻击利用许多计算机同时对目标站点发出成千上万个请求。为了避免被追踪，攻击者会闯进网上的一些无保护的计算机内，在这些计算机上藏匿DDoS程序，将它们作为同谋和跳板，最后联合起来发动匿名攻击.

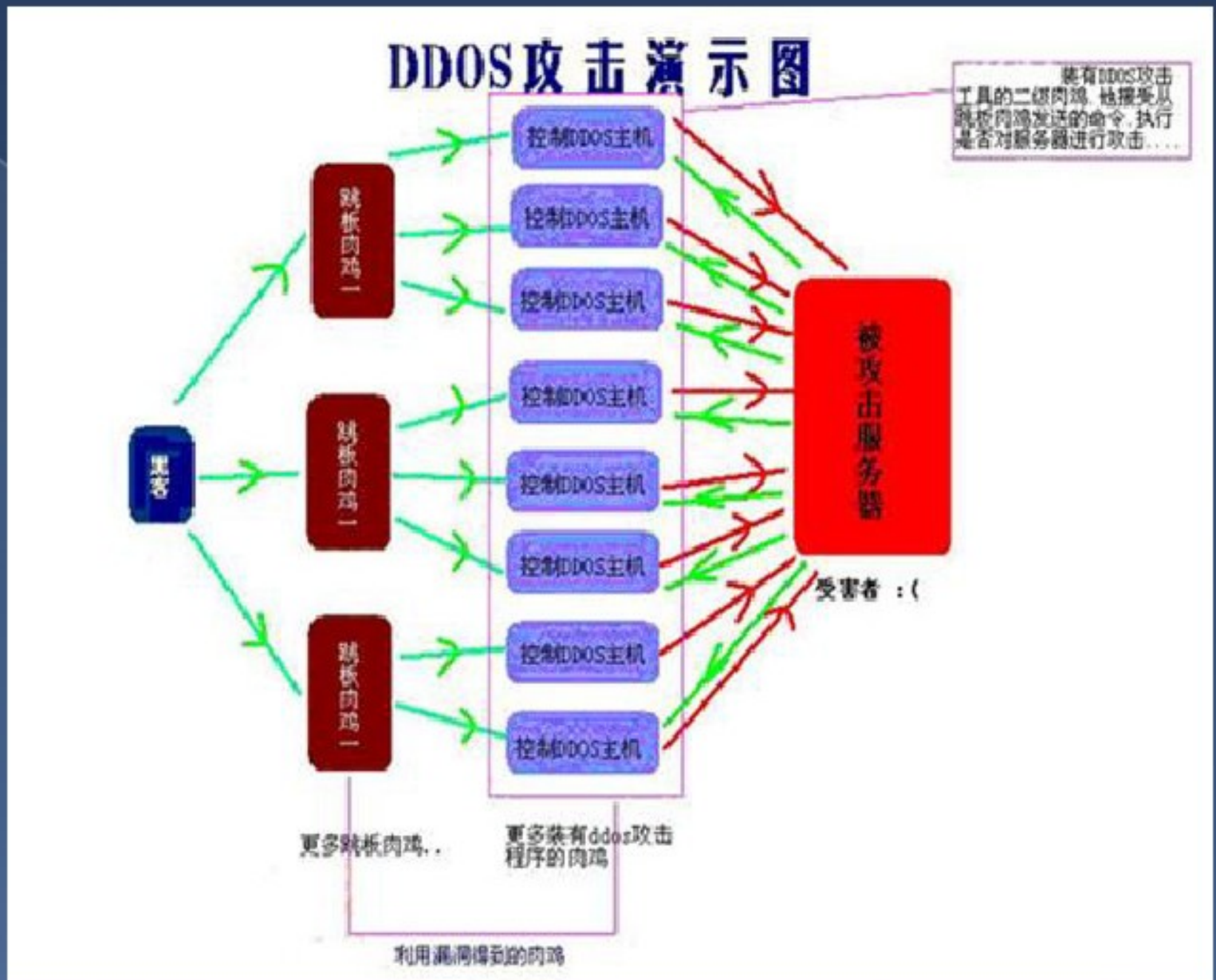

图2-1 DDOS 攻击演示图

2.3 DDOS的表现形式

DDOS的表现形式主要有两种：一种为流量攻击，主要是针对网络带宽的攻击，即大量攻击包导致网络带宽被阻塞，合法网络包被虚假的攻击包淹没而无法到达主机；另一种为资源耗尽攻击，主要是针对服务器主机的攻击，即通过大量攻击包导致主机的内存被耗尽或CPU被内核及应用程序占完而造成无法提供网络服务。

如何判断网站是否遭受了流量攻击呢？可通过Ping命令来测试，若发现Ping超时或丢包严重(假定平时是正常的)，则可能遭受了流量攻击，此时若发现和你的主机接在同一交换机上的服务器也访问不了了，基本可以确定是遭受了流量攻击。当然，这样测试的前提是你到服务器主机之间的ICMP协议没有被路由器和防火墙等设备屏蔽，否则可采取Telnet主机服务器的网络服务端口来测试，效果是一样的。不过有一 点可以肯定，假如平时Ping你的主机服务器和接在同一交换机上的主机服务器都是正常的，突然都Ping不通了或者是严重丢包，那么假如可以排除网络故障因素的话则肯定是遭受了流量攻击，再一个流量攻击的典型现象是，一旦遭受流量攻击，会发现用远程终端连接网站服务器会失败。

3 DDOS攻击的防御策略

由于DDOS的攻击具有隐蔽性，到目前为止我们还没有发现防备攻击的行之有效的方法。首先，这种攻击的特点是它利用了TCP/IP协议的漏洞，除非你不用TCP/IP，才有可能完全抵御住DDOS攻击。一位资深的安全专家给了个形象的比喻：DDOS就好象有1,000个人同时给你家里打电话，这时候你的朋友还打得进来吗？除加强安全防范意识，提高网络系统的安全性外，还可以采取下面几种安全措施:

用足够的机器承受黑客攻击。这是一种较为理想的应对策略。如果用户拥有足够的容量和足够的资源给黑客攻击，在它不断访问用户、夺取用户资源之时，自己的能量也在逐渐耗失，或许未等用户被攻死，黑客已无力支招儿。

和你的ISP协调工作，让他们帮助你实施正确的路由访问控制策略以保护带宽和内部网络。

在网络管理方面，优化路由和网络结构，经常检测网络安全设备配置信息，注意查看每天的安全日志。充分利用网络设备保护网络资源。所谓网络设备是指路由器、防火墙等负载均衡设备，它们可将网络有效地保护起来。当Yahoo！被攻击时最先死掉的是路由器，但其他机器没有死。死掉的路由器经重启后会恢复正常，而且启动起来还很快，没有什么损失。若其他服务器死掉，其中的数据会丢失，而且重启服务器又是一个漫长的过程，相信没有路由器这道屏障，Yahoo！会受到无法估量的重创。

关闭不必要的服务，限制同时打开的Syn半连接数目，缩短Syn半连接的time out 时间，及早发现系统存在的攻击漏洞，及时安装系统补丁程序。对一些重要的信息建立和完善备份机制，对一些特权帐号的密码设置要谨慎。

当你发现计算机被攻击者用做主控端或代理端时，要倍加留意。这说明攻击者已发现你的系统漏洞，要及时清除系统中存在的DDoS攻击的工具软件。

当你发现自己正遭受DDoS攻击时，应立即关闭系统，或至少切断与网络的连接，保存入侵的记录让安全组织来研究分析。

3.2 防火墙

防火墙就是一个位于计算机和它所连接的网络之间的软件。该计算机流入流出的所有网络通信均要经过此防火墙。防火墙对流经它的网络通信进行扫描，这样能够过滤掉一些攻击，以免其在目标计算机上被执行。防火墙还可以关闭不使用的端口。而且它还能禁止特定端口的流出通信它可以禁止来自特殊站点的访问，从而防止来自不明入侵者的所有通信。

3.4 使用专业DDOS防御设备

选择一款优秀的防黑安全产品。即配备监测工具，不断提高对系统的认识。无论是从网上下载公开源代码的监测工具，还是购买网络监测工具，都要实时监测别人是否在扫描自己的端口。若有人扫描端口，意味着有人可能要攻击此网络。譬如：万网使用的绿盟黑洞系统 黑洞目前分百兆、千兆两款产品，分别可以在相应网络环境下实现对高强度攻击的有效防护，性能远远超过同类防护产品。其使用多种算法识别攻击和正常流量，能在高攻击流量环境下保证95%以上的连接保持率和95%以上的新连接发起成功率。

黑洞主要作用：

a. 能够对SYN Flood、UDP Flood、ICMP Flood、HTTP GET Flood和(M)Stream Flood等各类DOS攻击进行防护。

b. 可以有效防止连接耗尽，主动清除服务器上的残余连接，提高网络服务的品质；可以抑制网络蠕虫的扩散。

c. 可以防护DNS Query Flood，保护DNS服务器正常运行。

d. 可以给各种端口扫描软件反馈迷惑性信息，因此也可以对其它类型的攻击起到防护作用。

3.5 ISP / ICP管理员

ISP / ICP为很多中小型企业提供了各种规模的主机托管业务，所以在防DDoS时，除了与企业网管理员一样的手段外，还要特别注意自己管理范围内的客户托管主机不要成为傀儡机。客观上说，这些托管主机的安全性普遍是很差的，有的连基本的补丁都没有打就赤膊上阵了，成为黑客最喜欢的"肉鸡"，因为不管这台机器黑客怎么用都不会有被发现的危险，它的安全管理太差了；还不必说托管的主机都是高性能、高带宽的-简直就是为DDoS定制的。而做为ISP的管理员，对托管主机是没有直接管理的权力的，只能通知让客户来处理。在实际情况时，有很多客户与自己的托管主机服务商配合得不是很好，造成ISP管理员明知自己负责的一台托管主机成为了傀儡机，却没有什么办法的局面。而托管业务又是买方市场，ISP还不敢得罪客户，怎么办？咱们管理员和客户搞好关系吧，没办法，谁让人家是上帝呢？客户多配合一些，ISP的主机更安全一些，被别人告状的可能性也小一些。

3.6 骨干网络运营商

他们提供了互联网存在的物理基础。如果骨干网络运营商可以很好地合作的话，DDoS攻击可以很好地被预防。在2000年yahoo等知名网站被攻击后，美国的网络安全研究机构提出了骨干运营商联手来解决DDoS攻击的方案。其实方法很简单，就是每家运营商在自己的出口路由器上进行源IP地址的验证，如果在自己的路由表中没有到这个数据包源IP的路由，就丢掉这个包。这种方法可以阻止黑客利用伪造的源IP来进行DDoS攻击。不过同样，这样做会降低路由器的效率， 这也是骨干运营商非常关注的问题，所以这种做法真正采用起来还很困难。

对DDoS的原理与应付方法的研究一直在进行中，找到一个既有效又切实可行的方案不是一朝一夕的事情。但目前我们至少可以做到把自己的网络与主机维护好，首先让自己的主机不成为别人利用的对象去攻击别人；其次，在受到攻击的时候，要尽量地保存证据，以便事后追查，一个良好的网络和日志系统是必要的。无论DDoS的防御向何处发展，这都将是一个社会工程，需要IT界的同行们来一起关注，通力合作。

结束语

以上就是对拒绝服务攻击方式进行了原理分析并提出了防御策略。随着电子商业的发展，DoS攻击将对我们的电子化社会产生更大的冲击。新的攻击方法必然还会出现，危害可能更大，需要我们进一步的研究。如果能时刻保持着警惕心理，采取必要的措施进行防御，就能将攻击带来的损失减少到最小，因此各种防御设备的安装也是有必要的。同时，拒绝服务攻击已经不仅仅是技术问题，也是一个社会问题，发挥社会和法律方面的作用打击网络犯罪，将会更加有效。其实，很多攻击方法并不新，存在时间也很长了（就像DoS），基本上人们对它们已经有所了解，只是当它被有恶意的人利用，破坏网络安全，人们才意识到问题的严重性。因此，人们应充分重视建立完善的安全系统，防患于未然。

谢谢观赏