计算机科学 2000Vol. 27№. 12

分布式拒绝服务攻击：原理和对策

Distrbuted Denial-of-Service Attack: Principle and Countermeasure

林曼筠 钱华林
（中国科学院计算技术研究所 中国科学院计算机网络信息中心 北京 100080）

Abstract Network security causes more and more attention today as the rapidly growing of Internet, and it even becomes the most important issue which must be settled before the technologies of Internet can be applied farther. Looking for all the possibility of network attacks and searching for the best countermeasure are a good way to improve the level of network security. In this paper, we study on the distributed Denial-of-Service attack and provide a set of countermeasures based on "baseline_value_overstep warning". We even address on the future forms of network attacks and its solvability at the end of this paper.

Keywords Network security, Network attack, Denial-of-Service attack, Distributed denial-of-Service attack

1 引言

随着网络技术的发展，Internet 正以迅猛强劲之势渗透到社会的各个层面，无论是在商业领域、教育科研机构或政府组织，人们日益感受到它的潜在魅力与巨大益处，从网上信息发布到电子商务，从个人主页到公司广告，从虚拟社区到政府上网，我们的生活和工作都因 Internet 而增添了新的内容和形式。Internet 设计的初衷是为了共享资源和交流信息，并没有充分考虑安全机制，网络世界的秩序在很大程度上依靠网民来自觉维护。然而频繁曝光的网络攻击事件表明，没有良好的安全保护措施，Internet 将无法获得真正深入和高层次的应用。

Internet 的发展带来了无国界的合作和交流，这种方便及时的交流在进一步加速网络技术发展的同时，也给网络上不安本分的入侵者提供了便利，使用简单而功能强大的新型攻击工具不断地被开发出来；同时，在 Internet 上，这些攻击工具随处可得，从而使一个没有专业知识的入侵者窃取或破坏一个技术先进的网络信息系统成为可能。深入分析现有的网络攻击方法，研究安全防御策略，对于提高网络安全，促进网络的健康发展有重大意义。本文在深入分析分布式拒绝服务攻击基本原理的基础上，提出了一系列预防和处理对策。

2 拒绝服务攻击

已知的网络攻击种类繁多，其中，拒绝服务攻击是一种操作简单而后果严重的网络攻击方法，分布式拒绝服务攻击更是代表了攻击手段发展的一种新的趋势，根据 CERT 的统计，自 1990 年以来，在各种网络攻击事件中，拒绝服务攻击所占的比例一直呈上升趋势。

攻击者通过某种手段，迫使被攻击目标（主机、其他网络设备或服务）丧失其"可用性"，这一类攻击方法统称为拒绝服务攻击。这是一种危害严重而且不容易预防的攻击方式。其原因在于攻击者的直接目的不是企图获得对目标的特许访问权限，而是滥用合法的访问权限努力耗尽目标的某种可用资源。

早期的拒绝服务攻击主要针对用户或主机，攻击者通常利用主机在用户认证、访问控制或应用程序等方面的漏洞获得对主机的非法访问，或者通过病毒感染的方法达到迫使主机无法提供正常服务的目的。但随着越来越多的人们对网络协议的深入研究和了解，拒绝攻击方法中引入了网络因素和分布式协同的概念。攻击者有可能利用网络协议或服务的弱点而无需特许的权限，在短时间内向被攻击目标发送大量貌似正常的数据包，为了响应这些数据包的请求或解析这些潮水般的无效数据包，目标消耗大量资源（CPU 处理能力、内存、带宽等），从而使其原本应该提供的服务的性能急剧下降，甚至因主机或网络系统崩溃而发生服务终止现象。基于网络的拒绝服务攻击常用的方法包括：ping of death、泪滴（Teardrop）、LandSlashdot 效应、UDP PACKET STORM、PING FLOODING、UDP FLOODING、TCP SYN FLOODING 以及 Smurf（直

接广播攻击)等。其中 Smurf 实际上是近年新出现的一种攻击工具的名称,它自动伪造 ICMP ECHO 请求数据包,以受害者的名义发往 IP 广播地址,从而使受害者在短时间内收到无数的 ICMP echo 回应数据包,以至使其所在网络发生拥挤甚至因带宽耗尽而瘫痪的现象。利用这类工具,攻击者发送一个数据包,受害者将收到某个网段上所有设备的回应,这种不对称的攻击方式又称为增量攻击。

第一个影响范围较大的拒绝服务攻击事件是 1988 年 11 月的 Internet 蠕虫(Internet Worm)事件,这个蠕虫程序利用操作系统的软件漏洞通过网络侵入 Internet 上的 UNIX 主机,并自动进行快速自我复制,被感染的计算机的处理能力很快被它的多个拷贝耗尽,无法用于正常用途。当时 Internet 上有六万多台主机,虽然被感染的仅有两千多台,但这期间,由于一时没有更好的防范措施,为了不被"蠕虫"感染,不少主机都以"拔掉网线"为对策,至使 Internet 几乎"关闭"了好几天。

3 分布式拒绝服务攻击

3.1 概念描述

90 年代后期,网络技术的发展日新月异,网络设施不断完善,新的网络应用层出不穷,然而先进的技术也不断地被加入网络攻击工具中。今年 2 月 Yaboo 等一些大型商业站点所遭受的分布式拒绝服务攻击,是继 Internet 蠕虫之后最引人注目的网络攻击事件,其攻击力度和范围之广都令人震惊,更让人担忧,与以前所有的攻击不同,受攻击者无法通过改善其防范措施来有效抵御这类攻击。这次事件充分证明了新式攻击工具的威力,也给我们带来新的启示:网络时代的安全,需要广泛的相互支持和协作。

所谓分布式拒绝服务攻击,其实是把客户/服务器的优秀体系结构、分层管理的优势和分布式处理的能力引入以往的拒绝服务攻击方法中,通过应用程序把分布在 Internet 上的一群主机组织起来,共同对一个或一组目标主机(网络)发起攻击,迫使目标资源竭尽,主机崩溃或网络拥挤堵塞,无法继续提供正常的服务。入侵者实施分布式拒绝服务攻击的主机群,称为分布式拒绝服务攻击网络。

资源总是有限的,无论你的系统如何健壮、资源如何充足,攻击者总是能够通过分布式拒绝服务攻击网络把许多零散、微不足道的资源组织起来,会聚成十倍甚至百倍于你的资源。如果你的系统每秒钟可以处理 10000 个请求,攻击者可以通过分布式拒绝服务攻击网络调用 100 台每秒发送 200 个请求的攻击代理来淹没你的系统。

3.2 结构和工作原理

Trinoo、TFN(Tribe Flood Network 三层洪潮网络)和 Stacheldraht(在德语中指"barbed wire",带刺的铁丝网)是用于分布式拒绝服务攻击的三组工具。对这些工具的分析结果表明,分布式拒绝服务攻击网络具有清晰的层次结构,如图 1 所示,它由分别位于攻击主

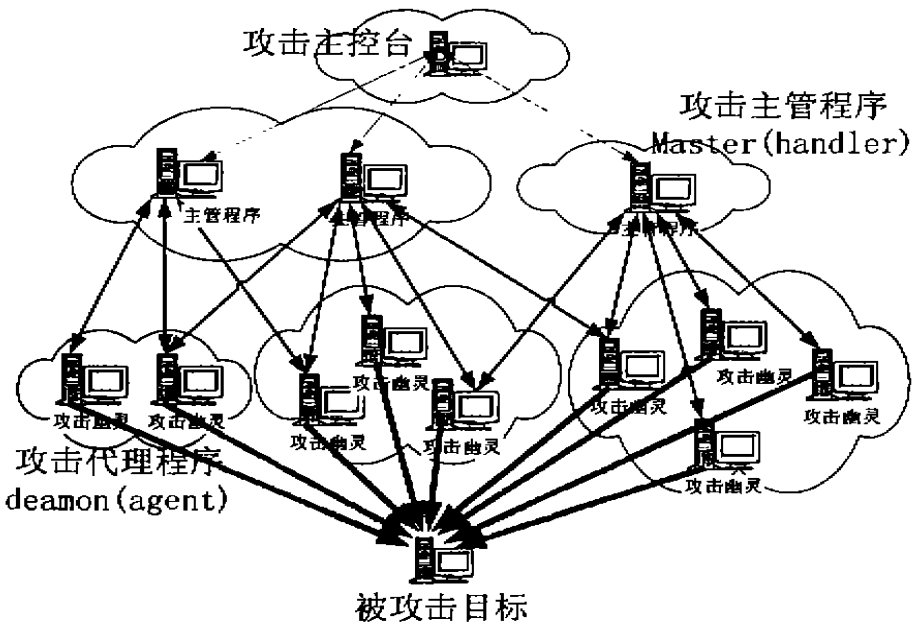

图 1 分布式拒绝服务攻击网络结构示意图

控层、攻击主管层和攻击代理层3个不同层次上的主机群组成。

攻击主控层位于最顶层、由攻击者直接控制的一个或多个攻击主控台构成，每个攻击主控台控制一个或多个攻击主管层节点。攻击主管节点(Master or Handler)位于中间层，每一个攻击主管节点负责管理其下层—攻击代理层的多个攻击代理节点(Deamon or Agent)，所有用于攻击的数据包，都由这些攻击代理节点上的攻击幽灵程序直接发出。通过这样一个三层结构的网络，攻击者通过一个攻击主控台，就可以操纵成百上千台Internet主机，使之同时向一个或一组目标发起攻击，而且，实际操作时，多个入侵者可以通过Internet或电话实时联络，使多个攻击网络同时工作。

3.3 通讯

攻击主管程序接受命令行方式的指令。在Trinoo中，攻击主控台通过Telnet方式与攻击主管节点取得联系，主控台每发送一个指令都携带有程序编译时设定好的口令，只有当主控台出示正确的口令，攻击主管程序才响应并执行命令；在TFN中，攻击主管程序可以把具有ROOT权限的远程SHELL调用绑定到某个端口上，以便攻击者用以输入控制指令，此外，攻击者也可以通过普通的TELNET或SSH等其他方式获得对主管节点的命令行访问权限，攻击者的控制指令无须提交密码即可被攻击主管程序执行；Stacheldraht是在参考Trinoo和TFN的基础上开发的，它最大的改进在于攻击主控台与攻击主管节点之间的通讯是经过加密的，攻击者通过一个专门的类似于TELNET客户端的应用程序访问攻击主管节点，交换的信息不但有口令保护，而且是通过对称密钥加密过的。

在Trinoo中，攻击主管程序与攻击幽灵(代理)程序之间通过指定端口的UDP数据包通讯，只有看到指定的密码时，攻击幽灵程序才会作出响应。TFN和Stacheldraht的攻击主管与攻击代理程序之间的通讯借助ICMP ECHO REPLY数据包实现，控制命令的类型由16位的报文标识栏以二进制数形式表示。尽管攻击主管与攻击代理程序之间的通讯是明文形式而且没有口令保护，但是，由于大多数的检测工具不显示ICMP数据包的数据部分，所以，其通讯还是很少被发现。Stacheldraht的攻击代理程序还能够与其主管程序相互配合，自动检测代理程序所在网络是否允许IP地址盗用。

3.4 攻击方法

攻击代理程序在接收到攻击主管程序发送来的攻击命令后，将按其指示的攻击目标、攻击时间长度以及攻击方法发起攻击。

Trinoo的攻击幽灵程序使用UDP洪潮的方法攻击目标；而TFN和Stacheldraht都可以选用UDP洪潮、TCP同步洪潮、ICMP ECHO请求洪潮、Smurfing这4种方法中的一种或多种，并且这4种攻击方法将与源IP地址盗用相结合，这一方面使攻击难以被跟踪，另一方面使目标收到的数据包更类似于正常情况。

3.5 安装

分布式拒绝服务攻击网络的安装过程包括一系列非常隐蔽的入侵攻击。通常的做法是，攻击者首先在某个具有高速的Internet连接、用户多而管理松散的主机上盗用一个帐户，用以存放预先编译好的扫描工具、入侵工具、Root Kit(用以隐藏入侵踪迹的工具)、Sniffer监听工具、分布式拒绝服务攻击的主管和代理程序，以及已经在控制之中的Internet主机(俘虏主机)的IP列表和具有可利用安全漏洞的主机(以下称脆弱主机)的IP列表。预先编译好的脚本程序能根据IP列表在俘虏主机或脆弱主机上安装分布式拒绝服务攻击的主管程序、安装完毕、则通过预先定义的端口自动建立与被盗用帐户所在主机的连接、或者向某个指定的免费Web Mail帐户发送电子邮件以确认安装成功。接着、攻击者根据攻击主管节点和俘虏主机、脆弱主机的分布情况，设计分布式拒绝服务攻击网络的分布图，编制脚本程序上载到被盗帐户中，该脚本程序将自动在入侵者指定的俘虏主机上安装攻击代理程序。

攻击者在每个攻击主管节点上维护一份由该主管程序控制的攻击代理节点的IP列表，在Solaris或Linux系统中，这个列表文件的名字一般为"…"。

在目前发现的分布式拒绝服务攻击网络中，攻击代理程序的自动安装程序会在系统的定时程序表(Crontab)中增加一条记录、设定攻击代理程序每分钟启动一次。在Stacheldraht中、攻击代理程序甚至可以按照攻击主管程序的指令，到某个指定的地方获取新的版本，进行自我升级。

4 安全对策

4.1 概述

分布式拒绝服务攻击之所以具有强大的攻击力，是与它先进的系统结构和庞大攻击阵容分不开的。以往的网络攻击借助系统在设计、配置、使用或其他管理方面的安全弱点而得逞，攻击者常常是单枪匹马发动攻势，而分布式拒绝服务攻击把分布式协作系统的思路带入攻击方法中，它不仅利用了单个系统的安全缺陷，更重要的是充分利用了Internet没有统一的组织和管理的弱点。即使你的局域网戒备森严，但只要Internet上还存在相当数量有安全隐患的网络、设备，分布式拒绝服务攻击的威胁就依然存在。

对付分布式拒绝服务攻击的最好的方法是"以其人之道还治其人之身"——以集体的力量挫败它。只有建立、完善 Internet 的整体安全体系结构，才能从根本上挫败分布式拒绝服务攻击。虽然建立 Internet 安全体系结构的种种努力都在进行当中，各个商业或公益组织的安全警告和对策也比比皆是，然而这一切都只能以建议的形式存在。由于 Internet 是一个自由组合的团体，总是存在无视这些建议的组织、网络或其他信息系统管理员、普通用户，因此，要实现 Internet 的整体安全，我们还有很长的路要走。

虽然不能彻底消除遭受分布式拒绝服务攻击的威胁，我们仍然可以采取一些措施，缓和分布式拒绝服务攻击的威胁。

4.2 紧密跟踪安全动态

这是一条普遍适用的原则，在技术飞速发展的今天，随时了解有关的安全动态更显必要。在今年 2 月，这些工具都只能运行于 Solaris 或 Linux 平台上，而 3 月，已经发现运行于 Windows 平台的 Trinoo 和 TFN2K。

随时掌握最新安全信息有三个主要目的，一是了解、掌握最新的安全保护技术、工具；二是了解新出现的安全漏洞或攻击方法，以及新的攻击工具的特点；三是根据对当前安全动态和自身网络、系统特点的综合分析，采取必要的措施增进网络、系统的安全，包括及时安装必要的补丁程序，修订原有的安全策略，引进必要的安全工具等等。

4.3 简单的服务，严格的访问控制策略

这个原则的指导思想来源于——越单一越安全。在网络边缘，即连接(不仅是物理，还包括逻辑连接)内部网络与外部网络的节点处，这个原则尤其重要。

简单的服务指仅提供必需的服务/功能，功能齐全是争取用户的一项重要措施，许多工具、产品的缺省安装都提供了名目繁多的功能，这些功能在方便用户的同时，也可能给攻击者带来了更多入侵的机会。严格的访问控制策略指：除非被明确允许，否则一律被拒绝。对于网络系统，这要依靠路由器等网络设备和防火墙、甚至是自主开发的一些安全工具来辅助实现。网络通讯是通过交换数据包实现的，所以应严格限制数据包的类型——除非在被明确允许的数据包类型之列，否则不允许进/出本网。这两项措施相配合，可以降低主机系统、网络系统的复杂程度，减小遭受未知模式攻击的可能性，不但减轻日常管理的工作量(比如需要审计的日志减少，系统配置时只需考虑为数不多的几类服务的特殊要求，等等)，而且一旦出现意外事件，实时搜查的范围小，便于迅速找到事情起因。

如果系统管理员可以在本地对网络设备进行配置、管理、就关闭其远程管理功能，以免入侵者利用其中某个还未公开的漏洞使你的系统成为他的俘虏；如果没有特殊的需要，可以设置路由器，使之阻隔来自外界的直接广播包，配置连网的主机设备，使之不响应发往广播地址的 PING 包，这可以使你的网络避免成为 Smurf 攻击的中转网络；使路由器仅允许源于内部的 IP 包向外发出，可以防止源于本网段的 IP 地址欺骗；严格配置的防火墙可以限制外部网络对内部主机、端口的访问，记录各种对系统的越权访问请求，这样的系统，能把入侵者的端口扫描拒之门外，即使网络中已经存在 stacheldraht 的攻击主管节点，攻击控制台也无法通过 16660 端口与其取得联系。

4.4 定期对系统进行安全检查

一般的系统日志仅提供有限的信息，所以，除了常规的日志审查之外，有必要定期对系统进行安全检查，安全检查的目的至少有两个：其一及时发现系统的安全缺陷，这些缺陷可能是业界新发现的，或者是由于系统配置改变引起的，或者是对系统的使用不当引起的；其二及时发现入侵的踪迹。

有两类工具值得推荐，一类是入侵检测工具，它能够实时检测入侵踪迹，通常也具有漏洞检测工具的功能，即通过模拟入侵行为，帮助管理员了解系统的安全漏洞所在；另一类是文件系统完整性检查工具，典型的有 Tripe Wire，它通过记录、比较文件或目录的 MD5 等多种难以仿冒的签名等信息，帮助管理员迅速发现被非法篡改的重要文件。需要提醒的是，对于记录文件/目录完好状态信息的签名文件，应该妥善保存，比如把它存放在一次性可写的 CDROM 上，以防被篡改。假如你的系统被悄悄地装上了 TFN master，并且其踪迹被 Root Kit 隐藏，你并没有注意到"…"的隐含文件已经存在于你的磁盘中，Tripe Wire 能迅速指出它的位置。

4.5 建立基准值超标报警机制

分布式拒绝服务攻击实际上包括两个阶段：准备阶段，即分布式拒绝服务攻击网络的安装阶段；主攻击发起阶段，即攻击者操纵分布式拒绝服务攻击网络，对目标发起后果严重而且立竿见影的攻击。

第一阶段的攻击受害者众多，而且入侵者为了隐藏踪迹，一般不会使被俘虏的系统受到显著的影响。尽管这一阶段的攻击悄无声息地进行，但是毕竟攻击程序存放并且运行于这些机器之上，所以无论是预防还是检测、清除工作都相对要容易得多，以上所列的几条措施对于避免成为第一阶段的受害者就十分有效。对于第二阶段的受害者，上述措施虽然能够在某种程度上减小分布式拒绝服务攻击对内部网络的影响，但是由于攻击是突发性的，事先没有任何预兆，而且难以区

分攻击数据流与正常数据流，因此没有卓有成效的对抗措施。

分布式拒绝服务攻击以耗尽目标的资源为直接目的，所以，借助性能监测工具，建立基准值超标报警机制，可以在意外事件发生时为管理员争取宝贵的处理时间，增强其应变能力。基准值应该包括带宽利用率、各类数据包的频率，各类数据包流量占总流量的比率，错误数据包的频率和类型分布等性能参数的统计平均值。这些数据值需要管理员使用性能管理工具在网络正常工作时多次测量得到。根据测量结果和网络、关键信息服务系统的资源供给的限制，确定适当的门限指标，当相应参数超标时，立即触发自动报警机制，进行报警，以便管理员及早发现拒绝服务攻击事件。比如，大量的 ICMP ECHO 数据包涌入网络可能是 Smurf 或 PingFlood 攻击的征兆，超量的 UDP 数据包，则可能预示着 UDP Flood。

4.6 准备简单实用的日志记录工具

实时日志分析是处理分布式拒绝服务攻击的主要手段，而常规的日志记录一般不能提供数据包的详细信息，也不能提供方便的检索和统计，所以管理员需要准备特殊的日志记录、分析工具。这些工具应该有源码，一方面为了安全起见，另一方面为了便于根据需要随时修改；另外，日志记录工具应该能够根据设置记录某些或所有数据包，能够记录数据包的指定部分或全部；日志分析工具则要求提供方便的检索、排序和统计功能，比如可以按照 IP 数据包的类型、IP 地址或子网掩码、TCP 或 UDP 端口等参数进行查询、排序和统计。当基准值超标或网络发生其他意外事件时，通过这个工具的统计分析，可以迅速定位可能引起麻烦的数据流，以便采取临时的堵截措施，缓和攻击带来的压力，争取宝贵的事件处理时间。也可以将取得详细的记录，迅速提交给安全顾问或 Cert 这样的安全急救组织，以获得支援。比如，当 ICMP ECHO 回应数据包频率超标时，应通过该工具查询这类数据包的数据部分及其源地址，一旦确认是 Smurf 攻击，立即阻隔相应子网甚至所有的 ICMP ECHO 回应包，并尽快联系发送回应包的子网，取得必要的支持和协作。

4.7 沉着处理意外事件

俗话说有备无患，有了上述的准备，再加上预先组织好的安全应急小组以及预先制定的安全处理流程、紧急求援联系表，就可以临危不乱，沉着应对分布式拒绝服务攻击。

如果发现你的系统已经成为分布式拒绝服务攻击的主管或代理节点，立即要做的事情是拔掉网线，然后才是其他的分析、处理。如果发现你的系统已经成为分布式拒绝服务攻击的主攻目标，则尽快借助日志分析工具、路由器等提供的信息，努力在入口信息超时失效之前回溯可疑数据包的来源。

结束语 分布式拒绝服务攻击代表了攻击工具演变的新趋势，它用以攻击的数据流更加复杂，更加逼真，难以使用"特征值"的方式描述。为此，除了选取一些行之有效的常规安全措施外，本文提出了一套安全策略——深入了解网络，广泛测定网络基准值，建立基准值超标报警机制，辅以特殊的日志记录、分析工具，使管理员能够及早预告网络攻击，争取更多的事件处理时间，努力减小甚至消除攻击的影响。

随着网络技术的发展，网络入侵工具的功能也不断加强，分布式拒绝服务攻击的出现表明，先进的客户/服务器结构、层次式体系及分布式处理能力一旦被用作攻击手段，其威力十分巨大。今天的入侵者能够设法调度 Internet 主机，也许将来他们会设法控制路由器等更加关键的设备，给 Internet 带来更大的威胁。网络安全是网络继续发展的基石，深入了解现有的攻击工具，分析网络攻击的未来发展趋势，积极寻求先进安全的主动防御措施，才能切实维护网络安全，这一领域还有许多工作需要我们去做。

参 考 文 献

1 Available at: http: // www. cert- org/incident-notes/IN-99-04. html, CERT Incident Note: IN-99-04, Distributed Denial of Service Tools

2 Available at, http: // www. cert org/advisories/ CA-2000-01: Denial-of-Service Developments CA-99-17-denial-of-service-tools. html

3 Available at, http: // www. cert org/reports/dsit-workshop. pdf "Results of theDistributed-Systems Intruder Tools Workshop"

4 David Dittrich's. Available at: http: // staff. washington. edu/dittrich/misc/
- The DoS Project's "trinoo"distributed denial of service attack tool
- The "Tribe Flood Network" distributed denial of service attack tool
- The "stacheldraht" distributed denial of service attack tool

5 RFC 2267-Network Ingress Filtering: Defeating Denial of Service Attacks which Employ IP Source Address Spoofing

6 Available at: http: // packetstorm. securify. com/distributed "Protecting against the unknown", by Mixter "Learning to cope with the SYNs of the Internet", by NightAxis & Rain Forest Puppy