典型的TCP/IP协议脆弱性及常见攻击方法分析

王晓薇，刘志宏，殷肖川，吴传芝
(空军工程大学 电讯工程学院，陕西 西安 710077)

摘　要:TCP/IP协议由于缺乏对安全性的考虑,存在一定的安全缺陷,给黑客攻击网络以可乘之机。文中首先对TCP/IP协议的脆弱性进行简要分析,然后对常见的攻击方法进行了详细介绍,并提出相应的防范措施。

关键词:网络;安全;TCP/IP协议;脆弱性
中图分类号:TP309　　**文献标识码**:A　　**文章编号**:1009-3516(2002)04-0046-05

TCP/IP协议[1]用于实现异种网络之间的互联,是当今世界上最流行的协议,除了最常用的TCP和IP协议外,还包含许多其他协议,如Telnet、FTP、SMTP等。由于TCP/IP协议形成于八十年代初期,设计上秉承简单实用的原则,因此在网络安全方面考虑有所不足(如TCP/IP协议数据流采用明文传输、缺少对数据的加密和认证等)。尽管TCP/IP技术获得了巨大成功,但也越来越暴露出安全上的缺陷。从CERT(Computer Emergency Response Team)2001年的报告中可以看出,利用TCP/IP协议进行的攻击日益增加。

1　TCP/IP协议的脆弱性[2]

1.1　不能提供可靠的身份验证

TCP/IP协议以32 bit的IP地址来作为网络节点的唯一标识,而IP地址只是用户软件设置中的一个参数,因而是可以随意修改的。对UDP来说,是根据这个IP地址来唯一标识通信对方。TCP则通过三次握手,使情况稍有改善。TCP中的每个报文都含有一个标识本报文在整个通信流中位置的32 bit序列号,通信双方通过序列号来确认数据的有效性。由于TCP设计三次握手过程本身并不是为了身份验证,只是提供同步确认和可靠通信,虽然这也能够提供一定的身份验证的支持,但这种支持很薄弱。首先,由于TCP/IP不能对节点上的用户进行有效的身份认证,服务器无法鉴别登录用户的身份有效性,攻击者可以冒充某个可信节点的IP地址,进行IP欺骗攻击。其次,由于某些系统的TCP序列号是可以预测的,攻击者可以构造一个TCP数据包,对网络中的某个可信节点进行攻击。

1.2　不能有效防止信息泄漏

IPv4中没有考虑防止信息泄漏,在IP、TCP、UDP中都没有对数据进行加密。IP协议是无连接的协议,一个IP包在传输过程中很可能会经过很多路由器和网段,在其中的任何一个环节都很容易进行窃听。更严重的是,现有大部分协议都是明文在网络上传输的,如telnet、ftp、smtp、pop3、http等,攻击者只需简单地安装一个网络嗅探器,就可以看到通过本节点的所有网络数据包。

1.3　没有提供可靠的信息完整性验证手段

在TCP/IP协议中,对数据完整性的保护也是比较弱的。在IP协议中,仅对IP头实现校验和保护。在UDP协议中,对整个报文的校验和检查是一个可选项,并且对UDP报文的丢失不做检查。

在TCP协议中,虽然每个报文都经过校验和检查,并且通过连续的序列号来对包的顺序和完整进行检查,保证数据的可靠传输。但事实上,绝大部分基于TCP的应用都假设TCP传输是可靠的,而实际上这种数据完整性的检查是不够的。校验算法中没有涉及加密和密码验证,很容易对报文内容进行修改,再重新计算

收稿日期:2002-01-05
作者简介:王晓薇(1972-),女,陕西富平人,讲师,硕士生,主要从事计算机信息对抗研究.

校验和。最后,TCP的序列号也可以任意的修改,从而在原数据流中添加和删除数据。

1.4 协议没有手段控制资源占有和分配

在传统的网络(如电讯网络)中,有两种控制资源占有和分配的手段:资源限额和计费。资源限额是一种主动的方法,即每个客户都分配一定限额,当资源使用达到限额时,通信活动就被限制。计费是一种被动的方法,即根据资源的使用事后向用户收取一定的费用,从而达到限制用户使用资源的目的。很多情况下,这两种方法是结合使用的。

然而,在TCP/IP中却没有提供相应的机制。TCP/IP中,设计的一个基本原则是自觉原则。如参加TCP通信的一方发现上次发送的数据报丢失,则主动将通信速率降至原来的一半。这样,也给恶意的网络破坏者提供了机会。如网络破坏者可以大量的发IP报,造成网络阻塞,也可以向一台主机发送大量的SYN包,从而大量占有该主机的资源(SYN Flood)。这种基于资源占用造成的攻击被称为拒绝服务攻击(DOS)。

2 常见TCP/IP协议攻击方法分析

下面对攻击者常使用的攻击方法进行简要分析,这些方法主要利用了TCP/IP协议中的局限性和内在的脆弱性。在分析的基础上提出相应的对策。

2.1 IP欺骗(IP Spoofing)

IP欺骗[3]是指一个攻击者假冒一个主机或合法用户的IP地址,利用两个主机之间的信任关系来达到攻击的目的,而这种信任关系只是根据源IP地址来确定。所谓信任关系是指当主机B信任主机A上的X用户时,只要X在A上登录,X用户就可以直接登录到主机B上,而不需要任何口令。如R-系列协议(包括rlogin、rcp、rsh)都可以利用主机之间的信任关系。

IP欺骗通常需要攻击者能构造各种形式IP数据包,用虚假的源IP地址替代自己的真实IP地址。如果主机之间存在基于IP地址的信任关系,目标主机无法检测出已经被欺骗。现在,已有很多可以发送伪造IP数据包的工具(如libnet),可以任意指定源IP地址。

IP欺骗的原理并不复杂,但真正实现起来却不是那么容易。一般而言,攻击者与目标主机和被假冒的主机不在同一个子网中,攻击者把伪造的IP数据包(包中的源IP地址是被假冒主机的IP地址)发送到目标主机,而目标主机的回应是发往被假冒主机,攻击者看不到,因此IP欺骗也称为是一种盲欺骗。为了假冒被信任的主机,攻击者首先要使被假冒的主机对目标主机发来的数据包不做响应。这可以通过SYN淹没来达到目的。此后,攻击者向目标主机发送建立连接的SYN数据包,再用猜测的序列号向目标主机发送ACK数据包。如果序列号猜测正确,目标主机就会接受ACK数据包。至此,TCP三次握手结束,一个TCP连接建立起来了。攻击者可以向目标主机发送命令,如在目标主机上安装后门程序或者窃取目标主机中的口令文件等。

要防止IP欺骗,对可以获得主机之间信任关系的命令必须采取限制措施,可以使所有R*的命令失效,移走.rhosts文件,清除UNIX系统中的/etc/hosts.equiv文件。其次,各个网络ISP应该限制源地址为外部地址的IP数据包进入互联网;合理的配置防火墙,限制数据包的源地址为内部网络的数据包进入网络。只有这样才能从根本上杜绝IP欺骗。

2.2 TCP会话劫持(TCP session hijacking)

TCP会话劫持主要是针对基于TCP连接的协议(如Telnet,rlogin,FTP等)发起的攻击。在这种情况下,攻击者与被假冒主机和目标主机之一在同一个子网中,攻击者通过一个嗅探程序可以看到被假冒主机和目标主机之间通信的数据包。

TCP会话劫持与IP欺骗不一样,IP欺骗是针对TCP三次握手过程进行的攻击,而TCP会话劫持跳过连接过程,对一个已经建立的连接进行攻击。攻击者看到被假冒主机和目标主机建立一个连接并进行身份认证后,通过对数据包捕获和进行分析,就可以得到连接的序列号。一旦得到正确的序列号就可以发送一个假冒的TCP分段,接管已经建立的连接。这样,被假冒主机发送的数据包都会被目标主机忽略,因为它们的序列号会被目标主机认为不正确(如图1所示)[4]。

通常,TCP劫持用来接管一个Telnet会话。Telnet是一个非常容易受劫持的协议,它在客户端和服务器端简单的传输字节流。攻击者只要将他们的指令插入被劫持的TCP数据段中,服务器就会把这个TCP段重装进指令串,并执行它。

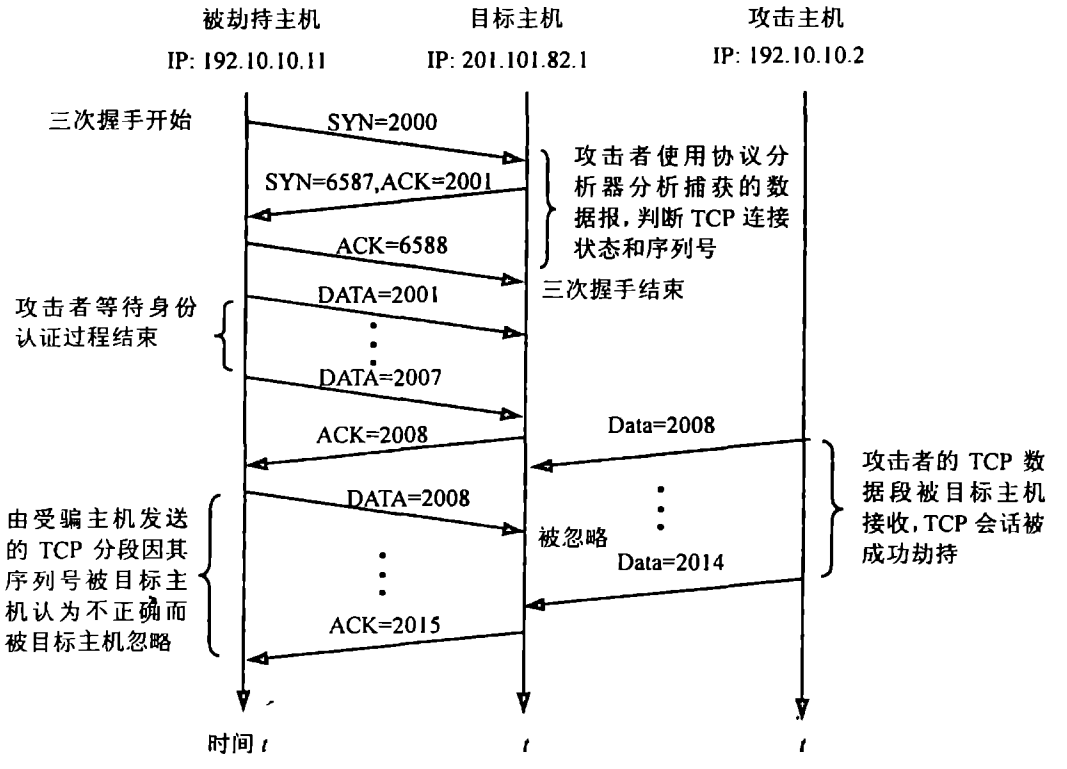

图 1 TCP 会话劫持

这种攻击方式可行的主要原因来自于 TCP/IP 协议本身的脆弱点,TCP 协议并不对数据报进行加密和认证,确认数据包的主要根据就是判断序列号是否正确。目前有多种软件可以进行 TCP 会话劫持,如 Hunt 等。

TCP 会话劫持是很难防范的。攻击者与被假冒主机和目标主机之一在同一个子网中,它可以看到被假冒主机和目标主机之间通信的数据包,从而得到正确的序列号。要防范这种攻击,最主要的方法是在传输层对数据进行加密。此外,把网络从共享媒体的网络(如 10BASE - T)向交换式网络迁移,使攻击者看不到其它网络数据流,这也可以减少会话遭到劫持的可能性。在主要的网段中安装入侵检测系统(IDS)也可以及时发现并防范这种攻击。

2.3 拒绝服务(Denial Of Service)

拒绝服务[5]的目的就是使受害的服务器不能提供正常的网络服务。攻击者可以通过多种手段达到这个目的。以下重点分析几种利用 TCP/IP 协议进行的拒绝服务攻击。

2.3.1 SYN 淹没(SYN Flooding)

SYN 淹没攻击[6]通过发送大量的 TCP SYN 连接请求,填满服务器的连接队列,使服务器不能对正常用户的 TCP 连接请求产生响应。1996 年两个最大最知名的地下黑客组织公布了可以进行这种攻击的原代码。正常情况下主机希望通过 TCP 连接交换数据必须经过"三次握手"(如图 2 所示)。首先 A 发送一个 SYN 数据包(一个具有 SYN 位的 TCP 数据包)给主机 B;主机 B 回答一个 SYN/ACK 数据包(一个具有 SYN 和 ACK 位组的 TCP 数据包)给主机 A,表示确认第一个 SYN 数据包并继续进行握手;最后主机 A 发送一个 ACK 数据包给主机 B,完成三次握手过程,这时如果主机 A 有数据就可以发给 B。这样通信双方正式建立一个连接,开始交换数据。

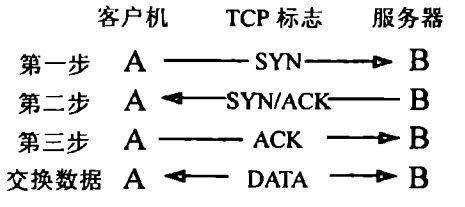

图 2 TCP 三次握手

SYN 淹没攻击以 TCP 三次握手协议为攻击目标,通过发送许多连接请求(SYN 分组)到目标主机的一个端口来进行攻击。为了保持匿名性,这些 SYN 分组通常使用假冒的 IP 地址。应答连接请求比产生分组需要消耗更多的 CPU 时间和存储空间,因为接收请求的主机需要记录关于新的连接信息并为连接数据分配存储空间。通过向目标主机连续发送 SYN 分组,最终将导致目标主机无暇处理来自合法用户的连接请求,直

至已建立的半开连接超时,并释放所占用的资源为止(如图 3 所示)。

要减少 SYN flood 攻击的影响。首先,阻止源 IP 地址为非内部地址的 IP 包进入互联网。这样,一个攻击者在多数情况下用自己的 IP 地址发送数据包时,就可以通过审计日志发现他们。其次可以增加额外的入侵检测工具。当然,增加请求队列的长度或当队列满时可以随意丢弃半开连接请求也不失为一个解决方法。

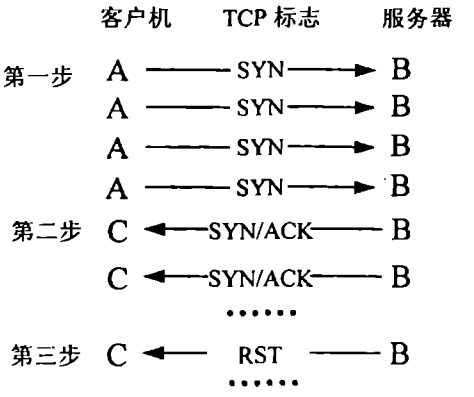

图 3　TCR SYN 淹没攻击

2.3.2　死亡之 Ping(Ping O'Death)

Ping 程序是通过发送一个 ICMP 回应请求消息和接收一个响应的 ICMP 回应来测试主机的连通性。通常也可以得到一些附加信息,如收发数据包的往返时间。死亡之 Ping 是利用 ICMP 协议的一种碎片攻击。攻击者发送一个长度超过 65 535 Byt 的 Echo Request 数据包,目标主机在重组分片的时候会造成事先分配的 65 535 Byt 字节缓冲区溢出,系统通常会崩溃或挂起(如图 4)。所有现代的操作系统和协议软件对 Ping O'Death 攻击都有免疫力,但是老的 Unix 系统可能仍然是脆弱的。

IP 数据包的最大长度是 65 535($2^{16}-1$) Byt,其中包括包头长度(如果 IP 选项未指定,一般为 20 Byt)。超过 MTU(Maximum Transmission Unit)的数据包被分割成小的数据包,在接受端重新组装。一般以太网的 MTU 为 1 500 Byt,互联网上的 MTU 通常是 576 Byt。ICMP 回应请求放在 IP 数据包中,其中有 8 Byt 的 ICMP 头信息,接下来是"Ping"请求的数据字节的数目。因此数据区所允许的最大尺寸为 65 535 - 20 - 8 = 65 507 Byt。

分段后的 IP 包要在接收端的 IP 层进行重组,这样"死亡之 Ping"就可以发送一个回应请求数据包,使它的数据包中的数据超过 65 507 Byt,使得某些系统的 IP 分段组装模块出现异常。因为在 IP 分段组装的过程中,它通过每一个 IP 分段中的偏移量来决定每一个分段在整个 IP 包中的位置,最后一个分段中,如果 IP 包的长度大于 65 507 Byt 各个分段组装后就会超过 IP 包的最大长度。某些操作系统要等到将所有的分段组装完后才对 IP 包进行处理,所以就存在这样一种内部缓冲区或内部变量溢出的可能性,这样会导致系统崩溃或重启。

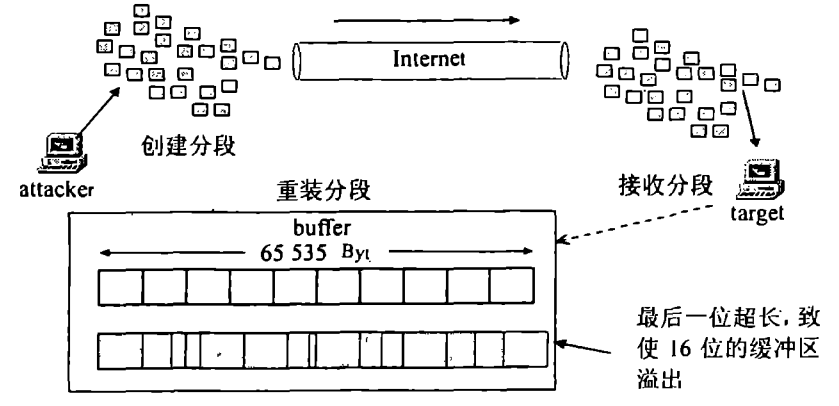

图 4　死亡之 Ping

这种攻击能使系统崩溃的原因因系统不同而异。有的可能因为内核中固定大小的缓冲区因 IP 数据包过大而越界,损坏了其它数据或编码;有的则可能因为用一个无符号的 16 bit 变量来保存数据包的长度和相关变量,当这些变量的值超过 65 535 Byt 时,变量不再与其数值一致 ,从而引发异常。要预防 Ping 死亡,首先应给操作系统打上补丁(patch)。其次,可以利用防火墙来阻止 Ping,然而这样也会阻挡一些合法应用。所以只要阻止被分段的 Ping,这样在大多数系统上允许一般合法的 64 Byt 的 Ping 通过,挡住了那些长度大

于 MTU 的 ICMP 数据包。

2.3.3 RST 和 FIN 攻击(RST and FIN attack)

在 TCP 包中有 6 个标志位来指示分段的状态。其中 RST 用来复位一个连接,FIN 表示没有数据要发送了。攻击者经常利用这两个标志位进行拒绝服务攻击。他们先分析通过目标主机和受骗主机之间的 IP 数据包,计算出从受骗主机发往目标主机的下一个 TCP 段的序列号,然后产生一个带有 RST 位设置的 TCP 段,将其放在假冒源 IP 地址的数据包中发往目标主机,目标主机收到后就关闭与受骗主机的连接。

利用 FIN 位的攻击与 RST 位的攻击很相似。攻击者预测到正确的序列号后,使用它创建一个带 FIN 位的 TCP 分段,然后发送给目标主机,好像受骗主机没有数据要发送了,这样,由受骗主机随后发出的 TCP 段都会目标主机认为是网络错误而忽略。

由于这种攻击需要分析目标主机和受骗主机之间发送的 IP 数据包,以决定正确的序列号,因此 RST 和 FIN 攻击只适用于机构的内部网。如果攻击者要在互联网上实施这种攻击,必须能够控制受攻击主机之间的路由节点,对于大多数的攻击者来说,访问这样的资源是不可能的。

象利用 RST 和 FIN 位进行的这种拒绝服务攻击是非常流行而且很恶毒的,它们或者中断或者完全拒绝对合法用户、网络、系统或其他资源的服务,对任何系统和网络都构成了严重的威胁。

3 结束语

本文通过对典型的 TCP/TP 协议的脆弱性和常见攻击方法进行分析,可以看出,要真正预防针对网络协议的攻击,需要从管理、技术和政策多方面来配合。希望随着网络安全技术的提高和 IPsec 的逐步完善,可以解决现存的一些 TCP/IP 协议问题。

参考文献:

[1] 谢希仁. 计算机网络[M]. 北京:电子工业出版社,1999.
[2] 赵海波. 网络防火墙的设计和实现[D]. 上海:上海交通大学,2000.
[3] 楚 狂. 网络安全与防火墙技术[M]. 北京:人民邮电出版社,2000.
[4] Harris B, Hunt R. TCP/IP security threats and attack methods[J]. Computer Communications, 1999, (22): 885 - 897.
[5] 卢津榕,冯宝坤. 解读黑客[M]. 北京:希望电子出版社,2001.
[6] 朱斌红、胡 明. 办公网络的信息安全模型研究[J]. 空军工程大学学报(自然科学版),2000,1(4):48 - 51.

(编辑:门向生)

The Analysis of Typical Fragility and Common Attack Methods of TCP/IP Protocol

WANG Xiao - wei, LIU Zhi - hong, YIN Xiao - chuan, WU Chuan - zhi
(The Telecommunication Engineering Institute, Air Force Engineering University, Xi'an, Shaanxi 710077, China)

Abstract: Since TCP/IP shows less consideration to security, some shortcomings in security are in existence, which provides Hacker opportunities to attack network. This paper first analyses the typical fragility of TCP/IP protocol, then puts emphasis on the analysis of the common attack methods and finally provides some useful safeguard measures.

Key words: network; security; TCP/IP protocol; fragility