TCP/IP 协议脆弱性分析

The Analysis of the Fragility of the TCP/IP Protocol

陆余良　李永祥　孙乐昌　朱俊茂

(解放军电子工程学院网络工程教研室　合肥230037)

Abstract　The fragility of the TCP/IP protocol coexists with its function. This article analyzes the principle of each layer of the TCP/IP protocol stack. And what's more, the author analysizes the possible fragility of the implementation and its probability of the usage by the hackers.

Keywords　TCP/IP, Fragility, Protocol

一、概述

传输控制协议/互联网协议(以下简称 TCP/IP)最初是为美国的 ARPANET 设计的,其目的在于能使各种各样的计算机都能在一个共同的网络环境中运行。经过二十多年的研究与发展,已充分显示出 TCP/IP 协议具有强大的连网能力。目前已形成了用 TCP/IP 协议连接世界各国、各部门、各机构计算机网络的数据通信网 Internet,TCP/IP 协议已成为事实上的国际标准和工业标准。

TCP/IP 实际上是一组协议的代名词,共分为四个层次。位于最底层的是链路层,也称为数据链路层或网络接口层,包括操作系统的设备驱动程序和网络接口卡,它们一起处理电缆或其它传输媒介的物理细节;链路层之上的是网络层(也称为互联网层),处理分组在网络中的活动,例如分组的选路。与其功能相适应,TCP/IP 协议族在此层中包括的协议有:IP 协议(互联网协议)、ICMP(网络控制报文协议)和 IGMP(Internet 组管理协议);再往上的是传输层,TCP(传输控制协议)和 UDP(用户数据报协议)是两个不同的传输层协议,TCP 为两台主机上的应用程序提供可靠的端到端的数据通信,UDP 则为应用层提供一种非常简单的数据传输服务。最上层是应用层,负责处理特定应用程序的细节,主要包括:Telnet(远程通信网络)、FTP(文件传输协议)、SMTP(简单邮件传送协议)、SNMP(简单网络管理协议)等。

TCP/IP 协议的设计与实现使不同计算机之间、不同操作平台之间的通信成为可能。但是,TCP/IP 协议是在网络规模不大、应用范围不广、计算机技术尚不够发达的情况下设计与实现的,当时的一种普遍认识是:安全性问题是上层的问题、与底层协议无关,因此 TCP/IP 在安全性方面做得不够完善。随着网络规模、计算机技术的日益发展,TCP/IP 存在的不可克服的脆弱性,越来越阻碍着 TCP/IP 的进一步广泛使用,也难以满足未来网络发展的需求。

二、链路层协议的脆弱性

链路层主要是为了发送和接收 IP 数据包、ARP 及 RARP 的请求与响应信息,因此这一层协议主要包括:

·以太网数据链路层协议,它是当今 TCP/IP 采用的主要的局域网技术。

·地址解析协议(ARP)。

·串行线路接口协议(SLIP)及点对点协议(PPP),用于连接广域网上的及拨号上网的两台计算机。

链路层上以太网技术发展比较成熟,目前用于远程工作站拨号上网的主要是 SLIP 和 PPP 协议,SLIP 协议是一种简单的帧封装方法,尽管仍在广泛地使用,但有一些问题:

(1)通信双方必须预先知道对方的 IP 地址,在建立过程中地址不能自动地设定。目前的 IP 地址已十分紧缺,这个限制也已成为主要问题,因为不可能给每个拨号因特网用户分配一个唯一的 IP 地址。

(2)数据帧中没有类型字段(类似于以太网中的类型字段),如果一条串行线路使用 SLIP 协议,则它不能同时使用其它协议。

(3)SLIP 不能进行任何错误检查和纠错工作,因而要到上层才能检测和恢复丢失帧、损坏帧或紧急帧。

(4)因为串行线路上的速率通常是较低的(<=19200b/s),而且通信经常是交互式的,所以在 SLIP 线路上有许多小的 TCP 分组进行交换。即使传输1个字节的小数据,也必须加上一个20字节的 IP 头和20字节的 TCP 头,因此信道利用率很低。

PPP(点到点)协议解决了以上的问题。PPP 协议处理错误检测,支持多种协议,在连接期间允许设定 IP 地址,允许身份验证,并在 SLIP 上做了许多其它改进。随着网络的发展,SLIP 协议将逐步为 PPP 协议所代替。

三、网络层协议的脆弱性

TCP/IP 在网络层中的协议包括：IP 协议、IGMP 协议、ICMP 协议。其中 IP 协议是核心，其它协议数据包也必须通过 IP 协议进行封装，因此，IP 协议的安全性影响着整个网络层协议的安全性。IP 主要存在以下几个方面的缺陷：

(1)IP Address 资源的日益匮乏　IP 地址是用来标识计算机所在的网络地址以及计算机本身的网络地址。IP 地址是32位二进制地址，它们通常用4个十进制的数表示，每组表示8位(1个字节)。每个字节表示的最大数目为255，因此，IP 地址的最大数目为40多亿。随着网络规模的日益扩大，网络上计算机的数目越来越多，IP 地址作为一种网络资源也面临着用完的问题。32位的 IP 地址已经不能满足 Internet 发展的需求。

(2)IP 地址的易欺骗性　在 IP 协议中，没有一种机制来检验数据包是否真正来自首部源 IP 地址对应的主机系统。在数据链路层中，网络接口卡的 MAC 地址是唯一的，因此在通常情况下，可以根据数据帧中的 MAC 地址与首部的 IP 地址相对应来确定 IP 地址是否真正来自它所代表的主机。但是在数据链路层中没有提供这样的机制来检验 MAC 地址与 IP 地址的一致性，而到了 IP 层，由于 IP 包中不包含 MAC 地址字段，因此它很难检验出其一致性。

这种缺陷的直接后果是 IP 地址易被盗用，如果用户 A 利用 SOCKET 编程直接向数据包中填写用户 B 的 IP 地址，并且数据包中包含攻击信息，则攻击信息到达目标系统后被入侵检测系统所截获，其获取的用户信息是用户 B 的 IP 地址。

(3)IP 源路径选项弱点　IP 源路径选项允许 IP 数据包自己选择一条通往主机的路径(选择经过路由的 IP 地址)。表面上看，IP 协议的这一功能没有什么漏洞，但如果与防火墙结合起来，则其漏洞是显而易见的。

防火墙允许一种调测包从外部网进入内部网，这种调测包就是利用 IP 协议的源路径选项的功能。当用户 A 想进入一个设有防火墙的内部网，与其中某一台主机 B 进行通信，如果它没有授权，当然无法进入。但是如果用户 A 在发送的请求报文中设置了 IP 源路径选项，使报文有一个目的地址指向防火墙，而最终目的是防火墙后的主机 B，当报文到达防火墙时将允许它通过，因为当数据包到达防火墙的 IP 层时，防火墙发现数据包的最终目的是主机 B，所以它将数据包重新发送到内部网中。IP 源路径选取项还可能导致目标系统被 IP 欺骗，这将在下面说明。

四、传输层协议脆弱性

TCP/IP 传输层协议为应用程序提供额外的通信服务，它主要包括以下三方面：

·传输层协议被封装在 IP 数据报中，并且它和其它层一起向应用程序提供所需的服务质量；

·用户数据报协议是简单的、基本的传输服务，它在传输数据时只增加了很少的控制开销；

·传输控制协议提供了一整套的服务来保障数据能准确地传送到目的地。

但是 TCP/IP 协议的传输层协议脆弱性已经成为网络协议攻击的主要突破口之一。在此主要以 TCP 协议为例，详细论述传输层协议的漏洞。

(1)TCP 连接的建立与终止　TCP 是一个面向连接的协议，无论哪一方向另一方发送数据之前，都必须先在双方之间建立一条连接。TCP 连接是通过所谓"三次握手"来完成的。图1描述的是 TCP 连接的建立与断开的过程。

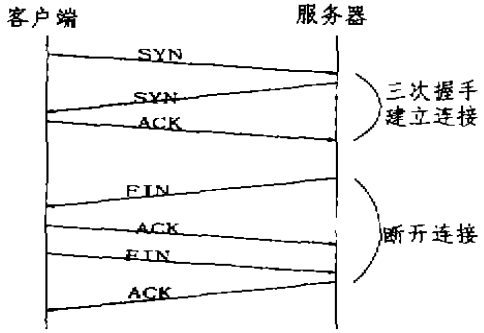

图1　TCP 连接的建立与断开

首先是客户端向服务器发出 SYN 报文请求建立连接，称为主动打开。如果服务器接受其请求，则向发出请求的客户端发送一个 SYN 报文，称为被动打开；客户端收到此 SYN 报文后再向服务器发送一个 ACK 报文，这样 TCP 连接建立起来了，客户与服务器之间就可以进行数据通信。当数据传送完成后，一方主动向另一方发出 FIN 信号，请求断开连接，另一方响应 ACK 信号，表示这个方向上的数据传输已经结束。但是，其反方向上的数据传输依然存在，只有当两个方向上都发送了 FIN 信号并得到对方确认后连接才真正断开。

TCP 连接的建立与断开机制保证了数据传输的可靠性与速度，但是随之而来的一个问题是：在连接建立过程中或完成之后，服务器端不再验证连接的另一方是不是合法的用户，这种脆弱性的直接后果是连接可能被窃取。

当合法客户 A 向服务器发送 SYN 报文，申请建立 TCP 连接，之后服务器向 A 发送回 SYN 包时，若此 SYN 包被一非法用户 B 截获，则它可以模仿客户 A 向服务器发送 ACK，完成连接，非法用户与服务器之

间建立起合法的 TCP 连接，而合法用户则仍在等待服务器对自己的 SYN 包的回应。

(2)TCP 连接请求队列　一个并发服务器调用一个新的进程来处理每个客户的连接请求，因此处于被动连接请求的服务器应该始终准备处理下一个连接请求。但是当服务器在创建一个新的进程时，或操作系统正忙于处理优先级更高的进程时，如果到达多个连接请求，仍有可能出现 TCP 采用以下规则处理的情况：

①. 对于服务器的每一个端口都保留一个连接请求队列，这个队列的最大长度可以根据服务器的性能及通信信道的带宽进行调节。当有新的连接请求到达通信端口时，则加入到队列的尾部，直到队列满；若传输层处理完当前事务，响应客户的连接请求时，则从队头调出一个连接请求进行响应，当它接收到客户的 ACK 信号后则表示连接建立已经完成，它会将此连接存放到②.所述的等待队列中。当连接请求超过75秒后未被传输层处理，则此连接请求超时，会被丢弃。

②. 对于每个端口还保存着另一个队列，此队列中保存的是已经建立但还未被应用层接收的连接。当应用层完成当前处理时，它会从此队列头部取连接进行处理。当连接75秒未被应用层接受则也会被应用层丢弃。

这种队列的处理方法看起来很适用于连接实际情况，但是很容易产生以下情况：如果某一用户不断向服务器的某一端口发送申请 TCP 连接的 SYN 包，但不对服务器的 SYN 包发回 ACK 确认信息，则连接无法完成。当未完成的连接填满传输层的队列时，它不再接受任何连接请求，包括合法的连接请求，这样就可能使服务器端口服务挂起。

(3)TCP 连接的坚持　所谓 TCP 连接的坚持是指当 TCP 连接上已经很长时间内未传送数据，但 TCP 连接仍旧能保持的特性。服务器会定时向客户端发送一个探测包来探测对方是否已经死机或重新启动。只要客户端机器未重起或死机，则它会一直保持着连接。

这样处理有一个最大的缺陷是 TCP 连接资源的浪费，毕竟服务器某个端口可以存在的最大连接数有限，当 TCP 连接不再传输数据而仍旧保持着，这将极大地降低服务器的性能。而且，如果在服务器的两次探测之间，使得某台机器伪装成服务器以前所连接的机器，则可以窃取 TCP 连接而与服务器进行通信。当然这样做的前提是使得原来与服务器连接的机器死机或重起。

五、应用层的脆弱性

TCP/IP 协议应用层的缺陷主要集中在 R 系列命令中。R 系列命令是指 rcp、rsh、rlogin 等命令。这些命令是基于可信任主机之间的关系而设置的方便用户登录的一种方法，可信任主机不需口令也可以通过 R 系列命令登录进目标系统。图2给出了利用 R 系列命令进行 IP 欺骗原理。

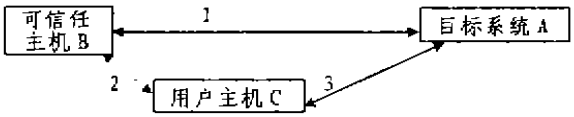

图2　利用 R 系列命令的缺陷进行 IP 欺骗

如果目标系统 A 的可信任主机 B 未启动或者已经被攻击死机，用户将自己的机器 C 伪装成主机 B，向目标系统 A 执行 R 系列命令，就可以以可信任主机的身份登录进服务器而不需要口令的验证。这种做法的唯一问题就是数据包序列号问题。两个系统之间利用 TCP/IP 进行数据通信，接收系统只接收序列号为它等待的序列号的数据包。因此如果用户主机 C 没有截获服务器上一个报文，就很难构造对服务器的回应报文。但是由于 TCP/IP 协议中序列号的规律性，有经验的用户即使不能截获服务器的数据包也可以猜测其序列号。

但是如果结合 IP 的源路径选项来进行上述操作，就可以不用猜测序列号。当用户从主机 C 模仿主机 B 向目标系统 A 发送请求报文时，可以将源路径选项中设置一个 C 的 IP 地址，这样根据源路径选项的含义，目标系统在回应报文时，也将设置此 IP 地址，即回应报文将从路径3到达主机 C，因此用户可以很容易地构造回应目标系统的数据包而冒充主机 B 与目标系统 A 建立连接。

TCP/IP 应用层的其它协议的漏洞主要是它们可以用来进入系统。如：我们可以利用 Telnet 应用程序登录进目标系统，之后，利用目标系统本身的漏洞(包括硬件和操作系统的漏洞)、运行一些程序，而获取超级用户权限。而利用 SNMP 协议构造网管数据包发给目标系统，根据目标系统的回应数据包可以获取目标系统的一些基本信息，如操作系统版本号，IP 地址、以及一些服务的版本号或是否开放了哪些端口等，为进入系统做准备。

参 考 文 献

1　[美]W. Richard Stevens 著. 范建华等译. TCP/IP 协议详解(卷1：协议). 机械工业出版社，2000. 4

2　[美]Craig Zacker 著. 王晓东等译. TCP/IP 网络管理. 中国水利水电出版社，1998. 8

3　[美]Pete Loshin 著. 沙斐等译. IPv6详解. 机械工业出版社，2000. 4