DOI: 10.19392/j.cnki.1671-7341.202116037

网络安全之 TCP/IP 协议

陈昱琦

重庆信息通信研究院　重庆　401336

摘　要: 随着计算机网络的快速发展,21 世纪已经进入了信息化时代。但随之网络安全问题也越来越突出,攻击者的破坏手段伴随着网络技术的发展更加高端,TCP/IP 协议是计算机计算和网络技术中最基本的协议。因此,研究 TCP/IP 协议,有效的解决协议威胁的问题,对计算机网络技术的发展非常重要。通过对 TCP/IP 协议进行概述,并分析当前 TCP/IP 协议存在的安全隐患和安全问题。比较分析后得出 IPv6 在安全性能上更由于上一代的 IPv4,极大地提高了网络的安全性。

关键词: 计算机网络; 网络安全; TCP/IP 协议

TCP/IP 协议作为计算机系统之间通信的技术规范,是当下网络技术所运用的主流协议。本文将详细介绍计算机网络以及 TCP/IP 协议族,使这些生活中常见的应用技术被更多了解,详见第一章、第二章。TCP/IP 协议的便利性使得在设计初期可以很好地被开发以及使用,但随着更加频繁的网络通信,各种网络协议所存在的安全漏洞也随之暴露。本文将简介 TCP/IP 协议族的基本原理与发展历史,并分析该协议族当前面临的安全问题,详见第三章、第四章。

1 计算机网络概述

计算机网络是指,由交换机、路由器等二三层网络设备通过物理线路相连所构建而成的基础网络设施,并向服务器、个人电脑等终端提供连接服务,使之通过网络设施实现相互通信。计算机网络的层次性是指,将网络的功能划分成若干个层次,每个层次负责独立的功能,低层次的网络功能为高层次的网络功能服务,高层次的网络功能依赖于低层次的网络功能。正是由于网络的分层,使得复杂的网络变得运行高效且利于维护。计算机互联的一个标准框架就是 OSI (Open System Interconnect) 参考模型,它是一个共计七层的标准框架,自下而上分别是物理层、数据链路层、网络层、运输层、会话层、表示层、应用层,如图 1 所示。

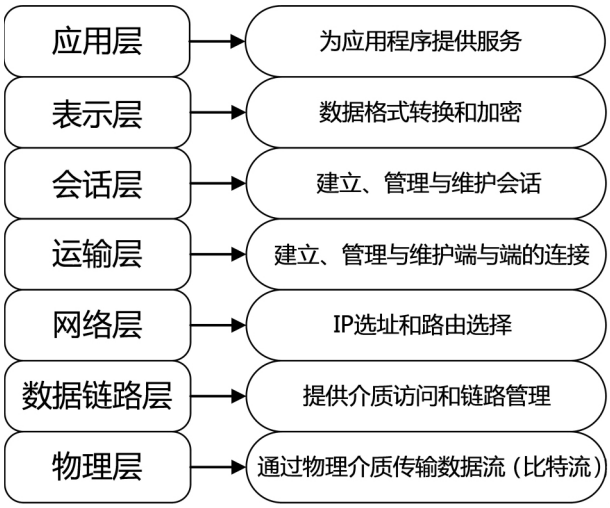

图 1 OSI 七层模型的划分

2 TCP/IP 协议

TCP/IP 协议并不完全符合 OSI 的七层参考模型,TCP/IP 协议将 OSI 的七层参考模型简化为四层,自下而上依次为网络接口层、网络层、传输层和应用层。每一层都需要它的下一层所提供的服务来完成自己的需求。

TCP/IP 协议族并不是单纯的 TCP 与 IP 这两个协议合并而产生的合称,而是指网络技术的整个 TCP/IP 协议族,又由于保障数据可靠传输的两个最基本的协议是 TCP 协议和 IP 协议,故称为“TCP/IP 协议”。IP 协议的功能是将数据链路层所封装出的“帧”同一转换为“IP 数据报”,使得数据可以在网络上进行三层路由转发,所以 IP 协议使各种计算机网络都能在因特网上实现互通。TCP 协议的功能是把数据切割为若干个数据包,并给每个数据包加上 TCP 包头,每一个包头都有源端口、目的端口以及各自的编号,数据的接收端可以根据包头中的编号来确定自己是否接收到所有的数据包,然后 IP 协议在 TCP 数据包封装 IP 报文头部,头部信息包含了数据的发送端和接收端的 IP 地址,有了接收端的 IP 地址,网络就知道了这个数据包想要去的目的地。如果在数据的传输过程中发生了数据丢失或失真等情况,TCP 协议会根据包头中的编号去请求数据重新传输,接收到重传的报文后重组数据。总之,IP 协议保证数据能传送到正确的目的地,TCP 协议保证数据传输过程中不出现丢失或破损。

2.1 TCP 协议

TCP 协议是面向连接的协议,一个完整的 TCP 连接建立过程如图 2 所示。为了在连接方和响应方之间可靠地传输数据,必须先在连接方和响应方之间通过三次握手的方式建立一条 TCP 连接。TCP 连接的建立过程大致为: 首先,连接方发送一个 SYN 标志位置位的 TCP 报文给响应方,SYN 报文中的信息包括连接方所使用的源端口号和响应方的目的端口号,以及该 TCP 连接的初始序列号 X; 然后,响应方在接收到该 SYN 报文后,返回一个 SYN 标志位和 ACK 标志位置位的报文,该报文的序列号为 X。最后,连接方也返回一个用于确认的 ACK 置位的报文给响应方,该报文的序列号为 X+1。至此,一个 TCP 连接成功。

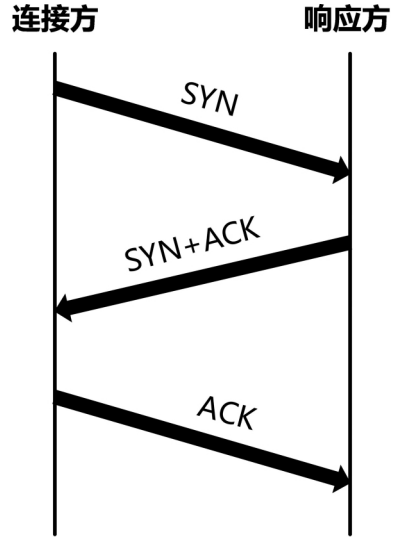

图 2 TCP 三次握手机制

2.2 IP 协议

IP 协议是 TCP/IP 协议族中的核心协议之一，它提供无连接的数据传输服务，它的主要功能有路由选择、寻址、分段以及组装。传输层将报文分成了若干个数据包，每一个数据包首先在源头的网关上进行路由匹配，然后一跳一跳地穿越若干个三层转发设备，最终送到目标主机。数据包在传输的过程中，由于物理层最大传输单元长度的要求，可能会被切割成若干小段，每一个小段都包含有完整的 IP 报文头部，但其中只有第一个小段包含了 TCP 头部。在穿越包过滤防火墙时，由于后续小段不包含 TCP 头部，将无法通过检测，在穿越状态检测防火墙时，则可以被检测通过。

IP 协议接收来自更底层发来的数据包，然后把数据包传递给更高的一层-TCP 层（传输层）。同样，IP 层也会接收来自 TCP 层的数据包，并传递给更底层。由于 IP 协议是无连接的，其无法确认数据是否有丢失或破损，所以 IP 数据包是不可靠的。

3 TCP/IP 协议的安全隐患

网络协议是计算机系统之间为了相互通信而共同遵守的技术规范。目前应用于互联网的主流协议 TCP/IP 协议族，由于在设计的早期过分注重其便利性和开发性，并没有足够考虑其安全性，因此安全问题普遍存在于很多的网络协议中。

3.1 TCP 协议的安全问题

第一是报文攻击：TCP 连接的建立是通过三次握手的机制来实现的，其中的第一条数据包为 SYN 数据包，第二条数据包是 SYN/ACK 数据包，第三条数据包是 ACK 数据包。在 TCP 连接关系里，一方为连接方，另一方为响应方，由于缺乏身份验证机制，可能会存在攻击方窃听响应方发送的 SYN 包的威胁；如果攻击方冒充连接方向响应方发出 RST 报文，然后发出 SYN 报文向响应方建立连接，攻击方则得到了制造破坏的机会，如果攻击方利用这个 TCP 连接持续发送危险数据，则会产生严重的后果。另外，攻击方还可以进行纯粹的破坏性攻击，比如攻击方可以同时冒充连接方和响应方，同时向连接方和响应方发送 RST 报文，连接方和响应方都以为 RST 报文是对方发来的，所以他们之间的 TCP 连接因此而断开，数据的传输也就必然中断。攻击方使用这样的方式持续阻断连接方和响应方之间的 TCP 连接，使得连接方和响应方之间的通信完全中断。第二是序列号攻击：TCP 连接最初的序列号是在发送 SYN 数据包时确认的，攻击方向响应方发送 SYN 报文获取上次的 ISN 数据，若攻击方获取了上次连接的数据，可以预测到后续的数据，那么攻击方就可以伪造有害数据并发给响应方，从而进行破坏。

3.2 IP 协议的安全问题

IP 协议在网络中提供了无连接的数据传输服务。IP 协议仅根据报文头部的目的地址信息进行转发，对 IP 报头中的源地址并不做任何检查。这就意味着，IP 协议默认认为，报头中的源地址是可以相信的、可以依靠的。因此，某些对访问请求来源敏感的服务可能会遭受非法入侵。即使网络中的防火墙限制了某些源地址去访问某些目的地址，但仍然无法避免攻击者冒用合法 IP 地址作为源地址，对服务器进行攻击。实际中，任何攻击者都能够利用 IP 协议不验证源地址真实性、合法性的缺点，自定义源 IP 地址来实现网络攻击，并且不会被发现。另外攻击者可以使用 IP 碎片攻击，由于 IP 协议无法检测源 IP 的合法性与真实性，攻击者可以向被攻击者发送大量的 IP 分片，被攻击者在收到这些大量的 IP 分片后，会对 IP 分片进行重组，重组大量的 IP 分片将大量占用被攻击者的计算资源，攻击严重的情况下，很可能会使得被攻击者陷入系统瘫痪。

4 基于 TCP/IPv4，v6 的安全分析

TCP/IP 协议族在设计上的先天不足使得其难以避免某些安全隐患，即使通过应用层的安全手段可以有效地避免一些底层的安全问题，但仍然无法彻底弥补其底层的先天不足。TCP/IPv6 的设计，充分总结了 TCP/IPv4 的安全问题并加以修复，使得 IPv6 的安全性更能满足当前网络安全防范的需求。除此之外，IPv6 宽广的地址空间、网络层的加密与校验等功能，使得其相较于 IPv4 的优势也更为明显。

5 结论

计算机网络的层次划分框架使得复杂的计算机网络系统易于实现以及维护。而网络协议，特别是 TCP/IP 协议簇保证了在通信过程中数据正确传输的重要协议。IP 协议使各种计算机网络都能在因特网上实现互通，TCP 协议保证了数据传输的正确性。但传统的 TCP/IP 协议由于过分强调其开发性和便利性，缺少安全性以及传输效率的考虑。新一代的 IPv6 在这两个方面的性能都显著提升。随着通信网络的发展，网络协议也许还存在一些其他的问题，但技术的发展就是不断地解决问题，在未来通信的效率会越来越高。

参考文献：

[1] 王雪晴. 计算机网络概述及与 SDN 的对比分析. 重庆邮电大学，2017.

[2] 刘宇峰. 新时期 TCP/IP 网络安全防范的应对措施探析. 中国联通，2016.