TCP/IP 协议与信息安全

陈彦君

（贵州大学科技学院 贵州贵阳 550003）

【 摘要 】TCP/IP 协议虽然存在着严重的安全隐患，但是仍然有着其自己独有的安全性。本文对 TCP/IP 协议工作原理进行了简要的介绍，讨论了 TCP/IP 协议在信息安全方面所具有的安全性与存在的安全问题，并对如何利用 TCP/IP 协议来保护信息安全进行了简要的探讨。

【 关键词 】TCP/IP 协议；信息安全；信息隐藏

TCP/IP Protocol and Information Security

Chen Yan-jun

（Guizhou University Institute of Science and Technology Guizhou Guiyang 550003）

【 Abstract 】TCP/IP agreement, although there are serious security problems, but still has its own security. In this paper, the TCP/IP protocol working principle were briefly reviewed in this paper, and discussed the TCP/IP protocol in information security is the safety and the safety of the existing problems. And to how the TCP/IP protocol to protect information security was briefly discussed in this paper.

【 Keywords 】TCP/IP protocol; information security; information hiding

0.引言

TCP/IP 协议是 Internet 上使用最流行的协议，如今已成为了 Internet 的一种标准，本文对 TCP/IP 协议的工作原理与安全性进行了简要分析。

1. TCP/IP 协议工作原理

1.1 TCP/IP 协议族分层

TCP/IP 协议族是由处于不同层次上的多个协议组合而成的。TCP/IP 与传统的 OSI 模型不同主要分为四个层次如图 1。

应用层
传输层
网络层
链路层

图 1 TCP/IP 协议族分层

每一层有着具体的功能。链路层有时也被称为网络接口层，主要包括操作系统中相关的设备驱动程序与计算机硬件中相对应的网络接口卡，共同对与电缆（或其他任何传输媒介）的物理接口细节进行处理。网络层主要是对分组在网络中的活动进行处理，在 TCP/IP 协议族中主要包括了 IP 协议、ICMP 协议以及 IGMP 协议。传输层的主要功能是为两台主机上的应用程序提供端到端的通信。在 TCP/IP 协议族中主要有两种互不相同的传输协议：TCP 协议与 UDP 协议。在应用层主要是对应用程序的的细节进行处理。

1.2 TCP/IP 协议主要工作流程

TCP/IP 协议主要工作流程如下（以文件传输为例）：

⑴ 源主机应用层将相关数据流传送给传输层；

⑵ 传输层将数据流进行分组，并加上 TCP 包头传送给网络层；

⑶ 在网络层加上包括源、目的主机 IP 地址的 IP 报头，生成 IP 数据包，并将生成的 IP 数据包传送至链路层；

⑷ 在链路层将 MAC 帧的数据部分装入 IP 数据包，然后将源、目的主机的 MAC 地址和帧头加上，并根据目的主机的 MAC 地址，将完整的 MAC 帧发往目的主机或者 IP 路由器；

⑸ MAC 帧到达目的主机后，在链路层将 MAC 帧的帧头去掉，并将去掉 MAC 帧头的 IP 数据包传送至网络层；

⑹ 网络层对 IP 报头进行检查，如果校验与计算结果不

(C)1994-2022 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

同，则将该 IP 数据包丢弃，如果结果一致就去掉 IP 报头，将 TCP 段传送至传输层；

⑺ 传输层对顺序号进行检查，判断是否是正确的 TCP 分组，然后再对 TCP 报头数据进行检查。如果正确就源主机发出确认信息，如果不正确或者是出现丢包，就想源主机发出重发要求；

⑻ 在目的主机的传输层将 TCP 报头去掉后根据顺序对分组进行组装，然后将组装好的数据流传送给应用程序。

2. TCP/IP 协议的安全性

TCP/IP 协议在设计之初没有对安全问题考虑很多，但是在安全性方面仍然有着其自身的优势。

首先，TCP 协议是面向连接的协议，指的是在进行通信前，通信双方需要建立起连接才能够进行通信，在通信结束后终止连接。当目的主机接收到由源主机发来的 IP 数据包后，会通过 TCP 协议向源主机发送确认消息。

同时在 TCP 协议中有一个重传记时器（RTO），源主机从 IP 包发送时开始计时，如果在超时前接收到了确认信号，计时器归零 如果计时超时，则表示 IP 包已丢失，源主机重传。利用这个计时器能够保证数据传输的完整性。TCP 协议为应用层提供了面向连接的服务，从而保证了网络上所传送的数据包被完整、正确、可靠地接收。

其次，利用 IP 协议进行信息传送，就像信息的明信片传送，对于运营商设备、协议乃至网络拓扑对用户均属开放可见。这也就是说，安全服务的提供不需要应用程序、其他通信层次和网络部件做任何改动。但是这种透明性也是容易被利用的一种安全漏洞。

3. 利用 TCP/IP 协议保护信息安全

虽然 TCP/IP 协议存在着较为严重的安全隐患问题，但是能够利用协议本身来实现信息隐藏，从而达到保护信息安全的目的。

对 TCP/IP 协议头数据格式进行分析，能够发现在这两个头结构中存在多个没有用于正常的数据传送或者是数据包的发送的区域。利用这些区域可以对数据进行保存和传送从而达到保护信息安全的目的。

当源主机与目的主机建立起 TCP 连接后，源主机就可以对要发送的数据进行编码转换，根据一定的算法将需要隐藏的数据装入到 IP 标识域内。而在目的主机则将所隐藏的数据分离出来，利用特定的编码算法对数据进行还原。

利用时间戳实现信息隐藏。时间戳是一个单调递增的值，从 TCP/IP 协议中可知，当一个数据分组穿过互联网时，时间戳选修会使得各个系统将它当前的时间标记在数据分组的相关选项中。

利用时间戳实现信息隐藏指的就是利用处理 TCP 包或者是 IP 包时所产生的轻微的延时来对 TCP 时间戳选项或者 IP 时间戳选项的低位段进行修改，当对协议的时间戳选项进行相应的修改后，根据 TCP/IP 协议的特点，会在网络中形成一个专门的信道来对隐藏信息进行传送。

参考文献

[1] 杨红敏.TCP/IP 技术浅谈 [J]. 科学之友，2011，(18)：16- 18.

[2] 季云龙，邵国强.TCP/IP 协议的网络安全[J].电脑学习，2011，(02)：29- 30.

[3] 吕涛，曹天杰.基于 TCP 协议的隐蔽通道研究[J].计算机安全，2010，(05)：51- 52，55.

作者简介：

陈彦君（1990-），男，贵州大学科技学院，在校学生，计算机科学与技术系。

(C)1994-2022 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net