信息安全丛书

Network Security Protocols

网络安全协议

原理、结构与应用

（第2版）

寇晓蕤　王清贤

高等教育出版社

网络安全协议

Wangluo Anquan Xieyi

原理、结构与应用

Yuanli Jiegou yu Yingyong

（第2版）

寇晓蕤　王清贤

高等教育出版社·北京

内容提要

信息安全包括三个分支：存储安全、传输安全和内容安全，本书重点关注传输安全，即利用网络安全协议保障信息安全。本书将网络安全协议定义为基于密码学的通信协议，抛开底层密码学的细节，从密码技术应用者的角度，讨论9个TCP/IP架构下具有代表性且应用较为广泛的安全协议（或协议套件），包括：链路层扩展L2TP、IP层安全IPsec、传输层安全SSL和TLS、会话安全SSH、代理安全Socks、网管安全SNMPv3、认证协议Kerberos以及应用安全DNSsec和SHTTP。

本书适合信息安全和相关专业的研究生使用，也可作为计算机、通信和密码学等领域研究人员、技术人员和管理人员的参考书。

图书在版编目(CIP)数据

网络安全协议：原理、结构与应用 / 寇晓蕤，王清贤著. -- 2版. -- 北京：高等教育出版社，2016.3
（信息安全丛书）
ISBN 978-7-04-044205-2

Ⅰ.①网… Ⅱ.①寇… ②王… Ⅲ.①计算机网络-安全技术-通信协议 Ⅳ.①TP393.08

中国版本图书馆CIP数据核字(2015)第270746号

策划编辑 冯 英　责任编辑 冯 英　封面设计 王 洋　版式设计 于 婕
插图绘制 杜晓丹　责任校对 陈旭颖　责任印制 刘思涵

出版发行 高等教育出版社
社 址 北京市西城区德外大街4号
邮政编码 100120
印 刷 山东临沂新华印刷物流集团
开 本 787mm×1092mm 1/16
印 张 25.75
字 数 510千字
购书热线 010-58581118
咨询电话 400-810-0598

网 址 http://www.hep.edu.cn
http://www.hep.com.cn
网上订购 http://www.landraco.com
http://www.landraco.com.cn

版 次 2009年1月第1版
2016年3月第2版
印 次 2016年3月第1次印刷
定 价 59.00元

物 料 号 44205-00

前　言

20世纪90年代中后期以来，信息安全一直是信息科学领域的研究热点之一。信息安全是一个庞大的领域，涉及技术、政策、人员、法律等多个分支，而本书关注技术内容。随着新技术的不断出现，信息安全的研究内容也在不断拓展更新。从保护的对象看，信息安全包括三个分支：存储安全、传输安全和内容安全，分别用于保护本地存储和远程传输的数据安全并防止或发现信息中出现非法或不良信息。本书主要论述传输安全，即利用网络安全协议保护通过网络进行传输的数据，确保其机密性、完整性、不可否认性，实现身份认证，并为实施访问控制提供支持。

本书定义网络安全协议为基于密码学的通信协议。鉴于已经有很多讨论密码学的专著，本书并不关注密码学的细节，而是将安全协议作为其应用者进行讨论。此外，本书讨论通信协议，这意味着每个协议都有明确的语法、语义和时序，它们体现的不仅仅是一种设计思想，而是与具体应用和特定的协议栈层次相关联。

网络安全协议已经在实际应用中发挥了重要作用。比如，IPsec除广泛用于VPN外，已经成为IPv6使用的安全方案；在网上银行及电子商务等领域，更是能随处看到SSL(TLS)的踪影。IPsec用于IP安全，SSL(TLS)弥补了传输层协议的安全性不足。除这二者外，TCP/IP协议族中的很多协议都有对应的安全协议标准，比如与DNS对应的DNSsec、与SNMPv1对应的SNMPv3等。

这种对应关系并不是偶然的，因为协议设计者们最初关注的焦点是网络的互连互通以及直观而便捷的网络应用。在这些问题得到很好的解决后，互联网的应用才能迅速普及。普及的同时安全问题浮出水面，并逐渐成为下一个焦点。在解决安全问题时，互联网的基础架构已经相当成熟并广泛部署，完全推翻这个已有的架构并不现实。可行的方案是针对各个协议进行安全修补，或者针对特定的需求设计新协议作为整个体系的补充。前一种方案的结果是衍生出IPsec等与已有协议对应的安全版本；后一种方案的结果是出现了用于代理的Socks、用于认证的Kerberos等协议。

无论从体系、理论还是应用的角度看，网络安全协议的发展都已经初具规模。虽然很多优秀的论著都涉及该方向，但相对信息安全领域的其他专著而言，国内外专门从协议的角度对其进行讨论的著作并不多见。

目前与安全协议有关的著作可归纳为以下几类：

1. 讨论网络安全，内容包括防火墙、IDS、防病毒等各项内容，网络安全协议只是其中的一个分支；

2. 密码学论著，内容包括各种密码算法，安全协议往往作为具体的应用实例；

3. 讨论安全协议的设计思想及分析方法；

4. 以某一个安全协议为主题进行讨论。

其中前三类论著往往仅涉及少数几个网络安全协议的思想，不涉及细节；最后一类则仅关注某个特定协议。第一和第四类论著适合计算机类的工程技术人员阅读，而第二和第三类论著则更适合密码学专业人员阅读。

本书从协议的角度展开讨论，目标是兼顾网络安全协议的体系及各个协议的细节，既包括协议设计思想，也包括具体流程和应用情况；同时面向具备计算机和密码学基础的读者，既能够用于教学，也能够为相关工程技术人员提供参考。

本书共9章，包括9个具有代表性且应用较为广泛的安全协议，并按照协议栈分层结构来组织。具体内容如下：

第1章概述，讨论相关的密码学基础、网络安全协议的引入、定义和设计思想。

第2章链路层扩展L2TP，讨论PPP协议，用于认证的PAP、CHAP以及相应的扩展协议L2TP。L2TP将“点到点”扩展到整个互联网范围，实际操作中既被单独使用，也经常与IPsec结合使用以构建VPN。

第3章IP层安全IPsec，讨论IPsec标准，涉及协商协议ISAKMP、IKEv1、IKEv2，数据处理协议AH和ESP以及实现和应用方式。

第4章传输层安全SSL和TLS，主要讨论SSLv3，并比较了它与TLS的差异。这两个协议都是对传输层安全的补充，前者为Netscape公司的版本，后者为IETF的标准。

第5章会话安全SSH，讨论SSH，包括其传输层协议、用户认证协议、连接协议以及相关应用。

第6章代理安全Socks，讨论Socks框架及Socks4、Socks5的细节，并讨论编程接口Socks5 GSSAPI。

第7章网管安全SNMPv3，讨论SNMPv3体系结构、基于用户的安全模型USM、基于视图的访问控制模型VACM以及报文序列化等内容。

第8章认证协议Kerberos，主要讨论Kerberos v5。在应用部分给出了Kerberos GSSAPI的细节，并讨论Windows认证模式。

第9章应用安全，讨论DNSsec和SHTTP。二者分别通过增加新的资源记录和新的HTTP首部引入安全特性。

在本书的组织结构上，参考TCP/IP的分层结构，按照由下向上的顺序，最先讨论网络接口层安全协议，最后讨论应用层协议。但我们建议读者在读完第1章后

将第2章放在第3、4、5、6、7章后阅读，这样条理会更为清晰。

本书第1版于2009年1月正式印刷出版。第1版编写之前，解放军信息工程大学信息工程学院网络工程系在2003年组织了“网络安全协议”讨论班，为本书第1版的编写打下基础。2004年开始，“网络安全协议”作为学院研究生选修课，面向计算机、网络、通信以及密码学等专业的学生开课，并作为有关培训班的必修课程。期间选修人数较多，学生反映好。本书的内容基于授课期间准备的素材，并且参考了学生的提问、建议及反馈。

2014年开始，作者着手对相关内容进行修订、更新，以期为读者提供一个内容更为严谨并能体现协议最新发展的版本。在第2版即将出版之际，作者感谢解放军信息工程大学网络空间安全学院一直以来的支持，感谢丛书编审委员会的专家，他们严谨认真的态度及客观诚恳的建议保证了本书的质量。

热忱欢迎广大读者批评、指导及交流，作者的电子邮箱为：kouxiaorui@263.net。

作者

2015年12月

目　录

第1章 概 述

网络信息安全问题是当前的研究热点。信息安全包括三个分支,即存储安全、传输安全和内容安全。通过因特网(Internet)进行信息交互是当前使用非常广泛的一种信息传输方式。传输控制协议/网际互联协议(Transfer Control Protocol/Internet Protocol,TCP/IP)是支撑互联网运行的基础,所有通过互联网传输信息的实体都必须遵守 TCP/IP 协议族的各项约定,而增强协议的安全性也就显得格外重要。

本章首先分析 TCP/IP 协议族中普通协议的安全缺陷及相应的安全需求,之后给出网络安全协议的定义以及建构这类协议所需的密码学组件。基于这些组件,讨论构建安全协议的一般方法,然后分析应用环境、协议栈层次以及安全性等因素对构建安全协议的影响。

1.1 网络安全协议的引入

从 20 世纪 90 年代开始,人们就已经深刻感受到了因特网给经济、生活、军事等领域所带来的巨大变革。因特网的出现、发展与 TCP/IP 协议族密切相关。20 世纪 70 年代末,TCP/IP 协议规范出台,IP 解决了异构网络互联问题,TCP 解决了可靠传输问题,它们为因特网的构建和运行提供了技术支撑;20 世纪 90 年代初,依托超文本传输协议(HyperText Transfer Protocol,HTTP)的万维网(World Wide Web,WWW)将因特网迅速推向大众;20 世纪 90 年代末,网际互联协议版本 6(Internet Protocol Version 6,IPv6)的出台则拉开了下一代互联网革命的帷幕。

与互联网迅速发展相随的是逐年递增的网络入侵事件,网络安全问题日益成为大众关注的焦点。2013 年网络安全领域最吸引眼球的爆炸性新闻莫过于斯诺登对于美国实施网络监控的爆料,这更加剧了互联网用户对于网络安全和个人隐私问题的关注。要列举影响网络安全的因素,从事不同工作的人员可能会给出不同的答案,比如:管理缺陷、人员误用、操作系统和应用程序漏洞等。本书从网络通信协议的角度来探讨安全问题。事实上,网络协议的设计缺陷是影响安全的重要因素之一。由于网络协议是整个网络通信系统的支撑,分析协议的安全缺陷并找

到相应的解决方案就显得尤为重要。

1.1.1 TCP/IP 协议族中普通协议的安全缺陷

TCP/IP 协议族出现之初,协议设计者主要关注与网络运行和应用相关的技术问题,安全问题不是重点。其结果是网络通信问题得到很好的解决,而安全风险却必须通过其他各种途径来防范和弥补。此外,因特网从诞生的第一天开始,就秉承开放的理念,而"开放"与"安全"、"隐私"永远都是一对矛盾。

网络协议是网络通信的基础,它规定了通信报文的格式、处理方式和交互时序,每一项内容都会影响通信的安全性。比如,如果协议规定的报文数据是明文形式,这种协议的报文就面临信息泄露的危险。下面讨论协议设计问题给通信系统带来的各类风险。

1. 信息泄露

网络中投递的报文往往会包含账号、口令等敏感信息,这些信息泄露的后果往往是灾难性的。即便没有这些敏感信息,用户也不希望自己的隐私被人窥探。但在因特网这个开放的环境中,用户在通信过程的控制方面显得无能为力。在将数据从源端投递到目的端的过程中,可能会经过隶属不同机构的网络,跨越不同的国家。在这个过程中,每一步都存在信息泄露的危险。

在众多的网络攻击方法中,嗅探是一种常见而隐蔽的手段。攻击者可以利用这种技术获取网络中的通信数据。在共享式网络架构下,所有数据都以广播方式发送,因此仅把网卡的工作模式设置为"混杂(promiscuous)",就可以嗅探网段内所有的通信数据。防范这种攻击的有效途径之一就是采用交换式网络架构,因为交换机具有"记忆"功能。它把每个端口①与该端口所连设备的物理地址进行绑定,并依据帧首部的"目标地址"把数据直接发送到相应端口,抛弃了共享环境下的广播方式。

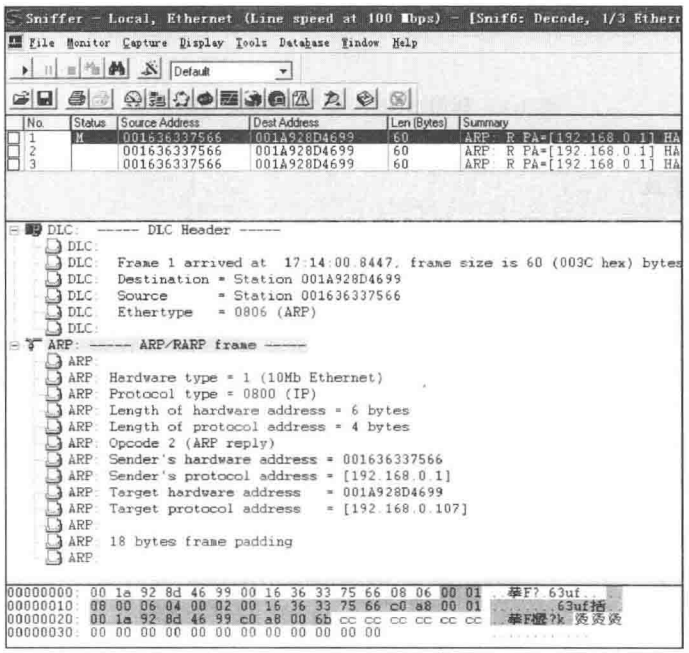
从防范嗅探的角度看,交换式网络环境似乎优于共享环境,但网络协议的设计缺陷却给它带来了另一种风险。地址解析协议(Address Resolution Protocol, ARP)是 TCP/IP 协议族中的一个重要协议,它实现了 IP 地址与物理地址之间的动态解析。在大多数操作系统实现中都设置了 ARP 缓存,用以提高通信效率。对网络通信而言,这种动态解析方式与缓存的结合充分体现了灵活性和高效性,是一种完美的解决方案,但对安全而言,却是一种灾难。

ARP 欺骗是攻击者在交换式网络环境下实施嗅探的基础。假设网络中有一台主机 H,它要嗅探 A 和 B 之间的通信数据。三台主机的 IP 地址分别为 IP_H、IP_A

① 端口的英文为"port",它既可以表示交换机等硬件设备的物理端口,也可以表示 TCP/IP 高层应用使用的软端口。此处是前一种含义,本书随后出现的"端口"都为后一种含义。

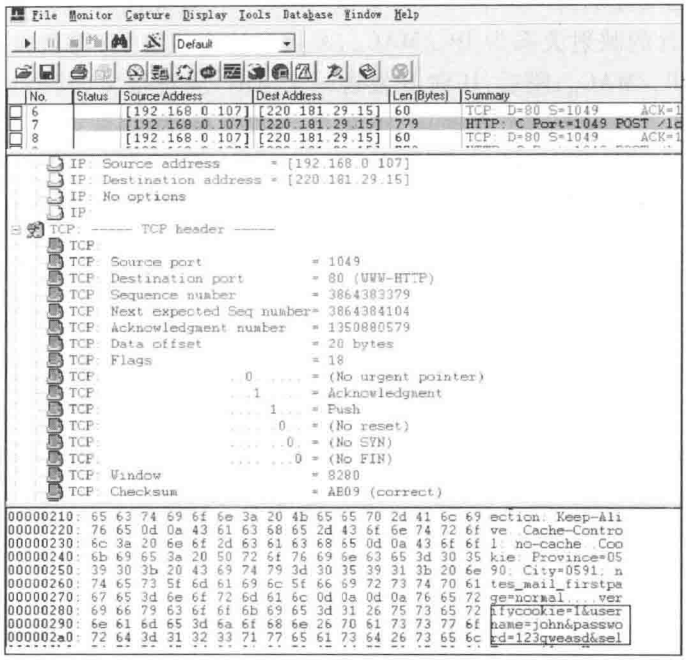
和 IP_B，物理地址分别为 MAC_H[①]、MAC_A 和 MAC_B。H 首先向 A 发送一个 ARP 应答报文，其中包含的映射关系为 IP_B/MAC_H，A 收到这个应答后，更新自己的缓存，保存映射关系 IP_B/MAC_H；随后，H 向 B 发送一个 ARP 应答报文，其中包含的映射关系为 IP_A/MAC_H，B 收到这个应答后，更新自己的缓存，保存映射关系 IP_A/MAC_H。至此，A 和 B 之间的所有通信数据都将发给 H。在截获了重要的通信数据后，H 可以把数据转发到正确的目的地，而 A 和 B 都无法察觉到嗅探行为。鉴于 ARP 缓存会定期更新，H 只要以小于更新时间间隔的频率发送 ARP 欺骗报文，就可以持续嗅探 A 和 B 之间的数据。

图 1.1(a)给出了 ARP 欺骗的一个实例。嗅探主机的 IP 地址为 192.168.0.111，物理地址为 00-16-36-33-75-66；实验网段的网关 IP 地址为 192.168.0.1，物理地址为 00-17-95-14-9C-88；被攻击的主机 IP 地址为 192.168.0.107，物理地址为 00-1A-92-8D-46-99。这个实例中，嗅探主机向被攻击的主机发送 ARP 应答报文，把自己的物理地址和网关的 IP 地址进行绑定，从而可以嗅探所有被攻击主机发往网关的数据。在图 1.1(b)中，可以明显看到用户使用 Web Mail 登录邮箱时使用的账号为“john”，口令为“123qweasd”。



(a)

① MAC：Media Access Control，介质访问控制。它和本节随后讨论的消息验证码缩写相同，但含义不同。



(b)

图 1.1 利用 ARP 欺骗实现嗅探功能示例

2. 信息篡改

除了信息泄露,信息篡改也是网络通信面临的一种安全风险。在信息泄露的例子中,攻击者若能成功实施基于 ARP 欺骗的网络嗅探,他就完全可以在转发数据之前对数据进行篡改。

从网络攻击的角度看,目前一种常用的攻击手段就是在截获的数据中插入一段恶意代码,以实现木马植入和病毒传播的目的。图 1.2 示意了一个被加入恶意

图 1.2 一个被插入恶意代码的 HTML 源文件示例