信息安全系列丛书

Network Security Protocols

Principles, Architecture and Applications

网络安全协议

——原理、结构与应用

寇晓蕤　王清贤

高等教育出版社

信息安全系列丛书

Network Security Protocols:
Principles, Architecture and Applications

网络安全协议

——原理、结构与应用

寇晓蕤　王清贤

高等教育出版社

内容提要

信息安全包括三个分支：存储安全、传输安全以及内容安全。本书关注传输安全，即利用网络安全协议保障信息安全。本书定义网络安全协议为基于密码学的通信协议。抛开底层密码学的细节，本书站在密码技术应用者的角度，讨论了九个 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。

本书适用于计算机、通信和密码学专业的读者，既可用于教学，也可为相关工程技术人员提供参考。

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．
—北京：高等教育出版社，2009.1
（信息安全系列丛书）
ISBN 978－7－04－025380－1

Ⅰ．网… Ⅱ．①寇…②王… Ⅲ．计算机网络－安全技术－通信协议 Ⅳ．TP393.08

中国版本图书馆 CIP 数据核字（2008）第 163568 号

策划编辑 陈红英 **责任编辑** 陈红英 **封面设计** 刘晓翔
版式设计 张 岚 **责任校对** 朱惠芳 **责任印制** 毛斯璐

出版发行	高等教育出版社	购书热线	010－58581118
社 址	北京市西城区德外大街 4 号	免费咨询	800－810－0598
邮政编码	100120	网 址	http://www.hep.edu.cn
总 机	010－58581000		http://www.hep.com.cn
		网上订购	http://www.landraco.com
经 销	蓝色畅想图书发行有限公司		http://www.landraco.com.cn
印 刷	国防工业出版社印刷厂	畅想教育	http://www.widedu.com
开 本	787×1092 1/16	版 次	2009 年 1 月第 1 版
印 张	24.25	印 次	2009 年 1 月第 1 次印刷
字 数	490 000	定 价	38.00 元

本书如有缺页、倒页、脱页等质量问题，请到所购图书销售部门联系调换。

版权所有 侵权必究

物料号 25380－00

信息安全系列丛书编审委员会

主　任：卿斯汉

副主任：陈克非　王清贤　王丽娜

委　员（按姓氏笔画排列）：

方　勇　吴　向　李凤华　何大可　张宏丽　张焕国
肖德琴　罗　平　杨义先　杨永川　周明全　林柏钢
赵一鸣　钮心忻　胡华平　贾春福　唐韶华　谢冬青
曾贵华　董晓梅

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，相关理论和技术已经逐渐成熟。信息安全包括三个分支：存储安全、传输安全和内容安全。本书关注传输安全，即利用网络安全协议确保信息的机密性、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。此外，本书关注通信协议，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)的身影。IPsec用于IP安全，SSL(TLS)弥补了传输层协议的安全性不足。除这两者外，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，因为协议设计者最初关注的焦点是网络的互联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。普及的一个结果就是安全问题浮出水面，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和用于认证的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，但国内外专门从协议的角度对其进行讨论的专著甚少。

目前与安全协议有关的专著可归纳为以下几类：

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；

试读结束：需要全本请在线购买：www.ertongbook.com

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、定义以及设计思想。

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，它通常与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、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，并比较了它和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。两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。在讨论SHTTP时，给出了CMS和MOSS这两种通用的报文安全封装方法的细节。

本书编写之前，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，为本书的出版打下基础。2004年开始，“网络安全协议”作为本院研究生选修课，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。

在本书即将出版之际，作者感谢解放军信息工程大学信息工程学院的支持，感谢国防科技大学胡华平教授的建议和支持。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。感谢高等教育出版社以及编辑陈红英女士，感谢参与本书校对的王佳杉先生。感谢信息工程大学信息工程学院研究生以及培训班学员的修改建议。

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

2008年8月

目录

试读结束：需要全本请在线购买： www.ertongbook.com

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。通过互联网(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。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。

本章将首先分析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构建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互联网给经济、生活、军事等领域所带来的巨大变革。互联网的出现和发展与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,它们为互联网的构建和运行提供了技术支撑;20世纪90年代初,依托HTTP的WWW将互联网迅速推向大众;20世纪90年代末,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。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。

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,每一项内容都影响了通信的安全性。比如,如果协议规定的报文数据是明文形式,这个协议的报文就面临信息泄露的危险。下面讨论协议设计不足给通信系统带来的各类风险。

1. 信息泄露

网络中投递的报文有时会包含账号、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。但在互联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,每一步都有信息泄露的危险。

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。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。

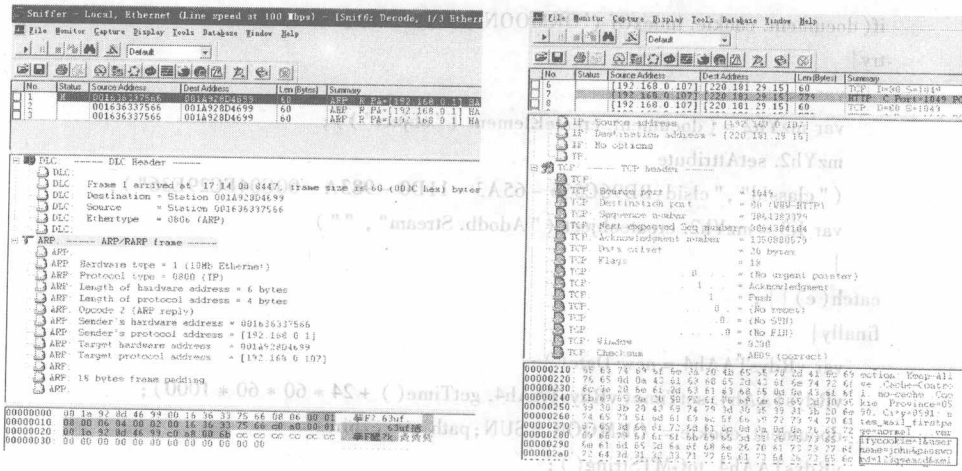
ARP 欺骗是攻击者在交换式网络环境下实施嗅探的基础。假设网络中有一台主机 H,它要嗅探 A 和 B 之间的通信数据。三台主机的 IP 地址分别为 IP_H、IP_A 和 IP_B,物理地址分别为 MAC_H②、MAC_A 和 MAC_B。H 首先向 A 发送一个 ARP 应答报文,其中包含的映射关系为 IP_B/MAC_H,A 收到这个应答后,更新自己的缓存,保存映射关系 IP_B/MAC_H;随后,H 向 B 发送一个 ARP 应答报文,其中包含的映射关系为 IP_A/MAC_H,B 收到这个应答后,更新自己的缓存,保存映射关系 IP_A/MAC_H。至此,A 和 B 之间的所有通信数据都将发给 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。

---

① 端口的英文词为"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"都指后一种含义。

② MAC:Media Access Control,介质访问控制。它与本节随后讨论的消息验证码缩写相同,但含义不同。

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) (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 示出了一个被插入恶意

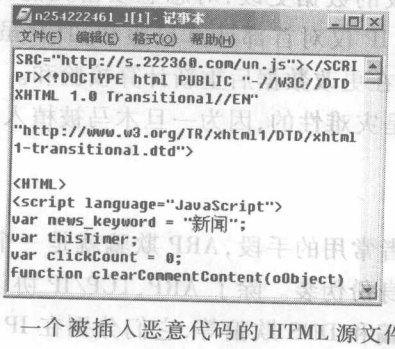


图 1.2 一个被插入恶意代码的 HTML 源文件示例

试读结束,需要全本请在线购买: www.ertongbook.com