网·络·安·全·实·用·丛·书

PRACTICAL NETWORK SECURITY TECHNOLOGY

网络安全基础与应用

张千里　编著

- 详细论述网络安全的**基础理论**
- 认真总结作者多年来的网络安全**建设经验**
- 准确介绍网络安全的**应用技术**及**前沿成果**

人民邮电出版社
POSTS & TELECOM PRESS

网络安全实用丛书

网络安全基础与应用

张千里　编著

人民邮电出版社
北京

图书在版编目（CIP）数据

网络安全基础与应用/张千里编著. —北京：人民邮电出版社，2007.7
（网络安全实用丛书）
ISBN 978-7-115-16029-4

Ⅰ. 网… Ⅱ. 张… Ⅲ. 计算机网络—安全技术 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2007）第 043889 号

内 容 提 要

本书的主要目的，就是结合网络安全系统构建的需求，介绍一些常见的网络安全措施。本书首先简要介绍了当前网络安全方面的一些基础知识，然后重点介绍了三个方面的主要内容——网络安全协议、系统安全防护、网络安全防护以及入侵检测和响应。网络安全协议所侧重的，是从协议的角度保护互联网络基础设施；系统安全防护指的是操作系统的安全防护；网络安全防护中重点介绍了网络安全管理政策、网络安全风险评估以及网络设备的访问权限控制；而入侵检测和紧急响应则侧重于从实际运营的角度来发现网络中的动态风险，并采取有效的措施。根据这些技术，基于开放源代码软件，一个廉价、可靠的网络安全解决方案就可以构建出来。

本书具有很强的实用性，通过本书的阅读，读者可以得到有关安全系统构建所需要的基本理论知识和实际技巧；另一方面，本书对于开源软件的侧重也是特色之一，开源软件，尤其是安全领域的开源软件，可以提供经济、可靠、安全的解决方案。因此，相信本书对于网络安全研究和从业人员，具有重要的参考作用。

网络安全实用丛书

网络安全基础与应用

◆ 编　　著　张千里
责任编辑　陈万寿

◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街 14 号
邮编　100061　　电子函件　315@ptpress com cn
网址　http://www ptpress com cn
北京隆昌伟业印刷有限公司印刷
新华书店总店北京发行所经销

◆ 开本：787×1092　1/16
印张：18
字数：437 千字　　2007 年 7 月第 1 版
印数：1－4 000 册　　2007 年 7 月北京第 1 次印刷

ISBN 978-7-115-16029-4/TN

定价：38.00 元

读者服务热线：(010)67129258　印装质量热线：(010)67129223

序

FOREWORD

随着互联网的普及和网络社会时代的到来，经济、文化、军事和社会活动将会强烈地依赖计算机网络，作为国家重要基础设施的网络的安全和可靠性问题已成为世界各国共同关注的焦点。而互联网的跨国界、无主管性、不设防、缺乏法律约束性，在带来机遇的同时也带来了巨大的风险。

网络安全的各种技术和协议，就是针对这一问题而深入的。多年来，网络安全的研究成果层出不穷，各种各样的工具也不断产生，全面地掌握这一学科，需要阅读大量的文献和长期的实践经验。

本书就是一本旨在概要介绍安全协议、技术及其实施的书籍。作者根据其多年来的网络安全建设经验，介绍了各个安全领域当中的一些重要的研究成果，并对这些成果的应用进行了简要的介绍。本书选材新颖、内容翔实、覆盖面广，既详细论述了网络安全的基础理论，同时又对网络安全的应用技术及研究前沿进行了准确的评价。全书层次结构清晰，行文流畅，篇、章相对独立，阅读容易。因此，相信本书会对网络安全研究和从业人员发挥应有的作用。

李　星

前 言

PREFACE

目前所运用的TCP/IP协议在设计时，安全并不是主要的考虑点。随着攻击技术的不断发展，各种各样利用网络底层协议本身的安全脆弱性进行攻击的手段层出不穷，而且其中很多是无法从根本上避免的。由于所有的应用协议都架设在TCP/IP协议之上，TCP/IP协议本身的安全问题，将极大地影响上层应用的安全。

网络的普及和应用，还是近十年的事情，而操作系统的产生要远早于此。在互联网络广泛应用之前的操作系统，主要面向个人用户或者是同一个组织里的用户，这与互联网络广泛应用之后的情况是完全不同的。很多操作系统缺省安装时存在大量的服务和缺省用户账号，即是明证。

随着整个社会的电子化进程的加速，这些网络安全风险正在成为实际应用中的问题，为了解决这些问题，网络安全技术不断地更新换代，各种新技术、新思路层出不穷。本书根据实际的需求，介绍其中一些相关技术，并通过使用开源软件，构建实际的安全系统。本书的第一章介绍计算机网络的安全风险。这部分介绍的缺陷包括：TCP/IP协议缺陷、软件实现缺陷和用户使用缺陷等。读者可以通过这个章节对计算机网络的安全问题有系统化的理解。这不但是网络安全初学者的一个较合适的入门，而且对网络安全的研究者也有一定的参考价值。本书的第二章侧重于介绍一些关于密码学的基础知识，这些密码学的常识是每个网络安全的从业者都应当了解的。在第三章中，我们介绍了在构建安全协议方面的几个有代表性的例子，从而让读者对于协议层安全防护有一个大概的认识。第四章介绍了两种主要操作系统，Windows 2000和UNIX/Linux的安全防护方法以及相应的常用安全工具，这部分内容对系统管理员有很好的参考价值。第五章介绍网络安全管理政策、网络安全风险评估以及网络设备的访问权限控制，这部分内容对网络管理员将有很大帮助。第六章的主要内容是入侵检测和响应，包括入侵检测系统的概念、技术和评估、入侵检测系统的发展前景、紧急响应的常用工具和方法。和其他安全技术相比，入侵检测系统是一个较新的技术。入侵检测系统既有很强的理论研究意义，又有很好的应用价值，是研究和开发网络安全产品的一个重点。如果防护和黑客的关系是“防护在明，黑客在暗”，那么检测和黑客的关系就是“黑客在明，检测在暗”。响应和恢复是发生安全攻击后的操作，只有进行了有效的恢复，才能保证系统不会被屡次破坏。第七

章介绍几个著名的开源软件的使用和配置。通过这些软件的安装和配置，一个简单的安全系统就可以构建出来。本书的最后一章讨论网络安全的未来。这部分主要根据作者在网络安全领域的研究和工作过程中所掌握的知识和经验，对网络安全的未来提出一些思考和建议。

承蒙清华大学电子工程系李星教授作序，特此致谢！

作　者

目 录

CONTENTS

第1章 因特网风险分析

CHAPTER 1

1.1 TCP/IP 协议的安全问题

TCP/IP 是目前因特网使用的协议，它之所以有今天这个辉煌的地位，是因为它在设计原则上所体现出众多优点，例如简单、易扩展、尽力而为等。这些原则给使用 TCP/IP 协议的用户带来非常方便的互联环境，使得因特网的用户以极快的速度迅速增加。但是，正是在这些优点的背后，TCP/IP 协议也存在着一系列的安全缺陷。而这些缺陷，是所有 TCP/IP 的实现所共有的，以下我们将简要介绍这些安全隐患。

1.1.1 TCP/IP 概述

1. TCP/IP 基本结构

TCP/IP 是一组 Internet 的协议，除了 TCP 和 IP 两个关键协议外，它还包括其他协议如 UDP、ARP、ICMP、Telnet 和 FTP 等。TCP/IP 的设计目标是将不同的网络进行互相连接，即实现因特网。为了达到这个目标，TCP/IP 被设计成四层结构，从上到下分别为：应用层、传输层、网络层和物理链路层，如图 1.1 所示。

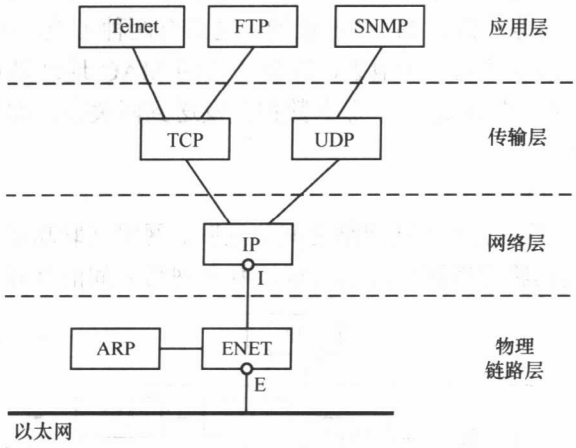

图 1.1 TCP/IP 基本逻辑结构

图中是 TCP/IP 协议层的逻辑结构。任何一台计算机想在因特网上与其他计算机通信，必须有这样的逻辑结构。每一层可以有一个或多个模块，每个模块实现一定的数据处理功能。应

用程序如 Telnet 和 FTP 运行在应用层。传输层给应用层提供端对端的数据传输，传输层有两种协议：TCP 和 UDP。网络层实现包转发功能，是网络之间互联的关键技术，网络层的协议为 IP 协议。物理链路层包括网络物理线路，网络驱动和一些协议如 ARP 协议。目前最常见的物理网络是以太网，ENET 模块是以太网的网络驱动。IP 模块下面的小圆圈是 IP 地址，ENET 模块下面的小圆圈表示 MAC 地址。IPv4 的地址是 32bit，目前正在推出 IPv6，其地址为 128bit。

TCP/IP 层次结构有两个重要原则：（1）在同一端点，每一层只和邻接层打交道，例如应用程序根本不关心网络层是怎么转发包以及数据在哪些网络上传输；（2）不同端点之间的同一层有对等关系。对等层之间可以进行通信，如应用程序之间的通信、TCP 模块之间的通信等。

2. TCP/IP 通信模型

通信模型是 TCP/IP 最基本的模型之一，它描述了端和端之间如何传输数据。在图 1.1 中，各层模块之间的连线表示数据流的路线。在发送端，数据从上层传到下层。对于使用 TCP 协议的程序，数据从应用程序流过 TCP 模块。对于使用 UDP 协议的程序，数据从应用程序流过 UDP 模块。数据单元每经过一个模块都被加上头信息标识该单元从哪来。在 TCP 和 IP 模块之间的数据单元叫做 TCP 包。在 UDP 和 IP 模块之间的数据单元叫做 UDP 包。在 IP 和 ENET 模块之间的数据单元叫做 IP 包。出了 ENET 模块，传输在电缆上的数据单元是以太网帧。

在接收端，数据从下层传到上层。每经过一个模块，数据单元都根据相应头信息的内容而被送到相应的模块，并且把相应的头信息去掉。在 ENET 模块，根据以太网帧中的协议项，决定数据被送到 IP 模块还是 ARP 模块。在 IP 模块，根据 IP 头信息中的协议项，决定数据被送到 TCP 还是 UDP 模块。在 TCP 和 UDP 模块，根据 TCP 和 UDP 头信息中的端口项，决定数据被送到哪个应用程序。

TCP/IP 提供两个主要的传输协议：TCP 和 UDP 协议。TCP 协议是一个面向连接的协议。它通过发送和确认机制，保证数据无错误传输。UDP 协议是无连接的，它只管发送和接收所有的包，不保证数据是否到达。使用 TCP 协议还是 UDP 协议由应用程序决定。例如 FTP 使用 TCP 协议，SNMP 使用 UDP 协议。

ARP 协议是地址转换协议，它把对方的 IP 地址转换成 MAC 地址，提供给网络驱动。因为以太网的帧能传到目的地是根据 MAC 地址的。这里有两种可能，如果目的地 IP 地址是本网络的，那么数据被直接发送到目的地去，即目的地的 MAC 地址是目的地的。另外，如果目的地 IP 地址不是本网络的 IP 地址，那么数据被发送到网关去，即目的地的 MAC 地址写的是网关的 MAC 地址。

3. TCP/IP 网络互联模型

TCP/IP 的另一个主要功能是不同网络之间的互联。网络互联功能在网络层实现，即一个 IP 模块连接到两个不同的物理链路层可以实现该两个网络之间的互联如图 1.2 所示。

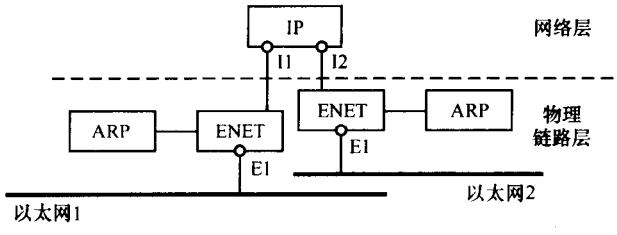

图 1.2　一个 IP 模块连接两个网络

图 1.2 是一个具有两个网卡分别连接到两个网络的网络层和物理链路路层结构。这样的结构可以实现包转发功能，即可以把来自一个网络来的包转发到另外一个网络去，网关和路由器都有这个功能。每个网络都有自己的网络驱动和 ARP 模块以及两个 MAC 地址，对应着两个 IP 地址。在 IP 模块，根据数据单元所标的目的地的 IP 地址，决定把数据送到哪个网络去。如图中两个网络的情况下，以太网 1 的数据可以传到以太网 2，反之亦然。这就实现了简单的网关功能。如果一个 IP 模块连接三个网络的情况下，来自一个网络的数据可以选择被送到其余的某个网络去，这就是路由选择功能。通过网关的数据转发和路由选择功能，就实现了不同网络的互联。

1.1.2 拒绝服务攻击

拒绝服务（Denial of Service，DOS）攻击就是消耗目标主机或者网络的资源，从而干扰或者瘫痪其为合法用户提供的服务。目前 DOS 攻击可以分为三类：网络带宽耗尽型、系统资源耗尽型以及处理缺陷型。带宽耗尽型主要是堵塞目标网络的出口，导致带宽消耗不能提供正常的上网服务。例如常见的 Smurf 攻击、UDP Flood 攻击、MStream Flood 攻击等。针对此类攻击一般采取的措施就是 QoS，在路由器或防火墙上针对此类数据流限制流量，从而保证正常带宽的使用，单纯带宽耗尽型攻击较易被识别，并被丢弃。资源耗尽型是攻击者通过严重消耗目的服务器关键处理资源，例如 CPU、内存等，导致目的服务器无法提供正常服务。例如常见的 SynFlood 攻击、Naptha 攻击等。以上两种攻击，都是利用系统对正常网络协议处理出现的问题，即使服务器或者网络都没有实现的问题，仍然可能会遭到攻击。而对于由于处理缺陷型的拒绝服务攻击，通常是由于系统在实现的过程中，引入了一些不必要的缺陷（bug），从而导致当攻击者使用某些异常流量时，系统会无法继续提供服务，这不在本部分讨论。

近年来，随着大规模攻击技术的发展，形成了一些分布式拒绝服务攻击（Distributed Denial of Service，DDOS）方法，它们利用多台计算机，采用了分布式对单个或者多个目标同时发起 DOS 攻击。DDOS 攻击为增加攻击威力，采用了许多新攻击技术，如伪造数据、消除攻击包特征、综合利用协议缺陷和系统处理缺陷、使用多种攻击包混合攻击、采用攻击包预产生法等来提高攻击的有效性。这种攻击通常会更难防治。

以下我们将简要介绍几种常见的由于 TCP/IP 协议问题造成的安全风险。

1. SYNFlood 攻击

最经典的攻击是 synflood 攻击，它利用 TCP/IP 协议的漏洞完成攻击。通常一次 TCP 连接的建立包括 3 个步骤，客户端发送 SYN 包给服务器端，服务器分配一定的资源给这个连接并返回 SYN/ACK 包，并等待连接建立的最后的 ACK 包，最后客户端发送 ACK 报文，这样两者之间的连接建立起来，并可以通过连接传送数据了。而攻击的过程就是疯狂发送 SYN 报文，而不返回 ACK 报文，服务器占用过多资源，而导致系统资源占用过多，没有能力响应别的操作，或者不能响应正常的网络请求。

这个攻击是经典的以小搏大的攻击，自己使用少量资源占用对方大量资源。一台 P4 的 Linux 系统大约能发 30～40Mbit/s 的 64 字节的 synflood 报文，而一台普通的服务器 20Mbit/s 的流量就基本没有任何响应了（包括鼠标、键盘）。而且 synflood 不仅可以远程进行，还可以伪造源 IP 地址，给追查造成很大困难，要查找必须对所有骨干网络运营商的路由器一级一级

地向上查找。

针对 Synflood 攻击，常见的解决方法有路由器限速以及 SynCookie。路由器限速就是限制 SYN 包的到达速度；SynCookie 方法则是在建立 TCP 连接时，要求客户端响应一个数字回执，来证明自己的真实性，从而解决了目标计算机系统的半开连接队列的有限资源问题。

2．Naptha

由于对于每个建立的 TCP 连接，系统都要耗费相对较多的资源，因此如果同服务器建立大量的 TCP 连接，服务器则会由于资源耗尽而无法响应其他的用户。这一想法的问题在于，如果使用通常的 API，在服务器无法响应之前，攻击者就已经崩溃了。因此，Naptha 不使用传统的网络 API 来设置 TCP 连接，不像真实的 TCP/IP 堆栈那样，它不保存任何连接状态的记录，它只根据发给它的报文中的某些标志来进行响应。按照这种方法，它可以与目标主机建立成千上万的连接，而与目标主机相比，攻击者只使用了很少的资源。使用这种方法，它可以对目标主机上的某个特定服务或 TCP/IP 堆栈自身造成真正的威胁。Naptha 攻击可以通过分布式的方式来实现，因此使其变得更为有效。

攻击的第一步要从一个伪造 IP 地址的所有可能端口向目标主机发送一系列的 SYN 报文。然后需要在伪造 IP 所在的局域网中运行一个程序，确保路由器的 ARP 表中有这台“虚拟主机”（就是伪造的 IP 地址）。接下来，它会监听从目标主机发往虚拟主机的报文。这个程序会使用合适的标志以及序列号来响应那些报文从而建立连接。使用虚拟主机主要是为了让跟踪攻击来源更为困难。

总之，Naptha 攻击表明了资源耗尽攻击的严重性。针对这个问题，还没有一个显而易见的解决方法。

3．流量放大器

流量放大器经常被用于实施分布式拒绝服务攻击。所谓的流量放大器，就是说当攻击者输入流量会经过这一系统的处理而放大几倍，这样如果攻击者发送大量的源地址被修改为要攻击的系统的流量到这些放大器时，就会出现大量的流量到目的系统，从而导致拒绝服务攻击。

Smurf 攻击是以最初发动这种攻击的程序名 Smurf 来命名的。这种攻击方法结合使用了 IP 欺骗和 ICMP 回复方法使大量网络数据包充斥目标系统，引起目标系统拒绝为正常系统进行服务。攻击者向一个具有大量主机和因特网连接的网络的广播地址发送一个欺骗性 Ping 分组（echo 请求），这个目标网络被称为反射站点，而欺骗性 Ping 分组的源地址就是被攻击的系统。如果路由器接收到这个发送给 IP 广播地址（如 202.112.0.255）的分组后，将它映射为以太网广播地址 FF:FF:FF:FF:FF:FF，就会对本地网段中的所有主机进行广播。而所有的 ECHO 包则会被转给被攻击系统，当攻击者使用大量的反射网络的时候，就会导致被攻击系统由于缺少可用的网络带宽而丧失服务能力。

另外一个常见的手段就是利用 DNS 服务器的 DNS 查询。攻击者向多个 DNS 服务器发送大量的查询请求，这些查询请求数据包中的源 IP 地址为被攻击主机的 IP 地址，DNS 服务器将大量的查询结果发送给被攻击主机，使被攻击主机所在的网络拥塞或不再对外提供服务。

对于这些攻击来说，基于路由器的ACL 和限流是比较有效的防范措施。此外，对于 Smurf 攻击，可以配置路由器不转发来自外网的针对广播地址的数据包。

4．OSPF 的攻击

OSPF（Open Shortest Path First）是使用于自治域内部的另一种路由协议。OSPF 使用的路由算法是状态连接（Link - State）算法。在该算法中，每个路由器给相邻路由器宣布的信息是一个完整的路由状态，包括可到达的路由器、连接类型和其他相关信息。和 RIP 相比，OSPF 协议中已经实施认证过程。但是该协议还存在着一些安全的问题。

LSA（Link State Advertisement）是 OSPF 协议中路由器之间要交换的信息。一个 LSA 头格式如图 1.3 所示。

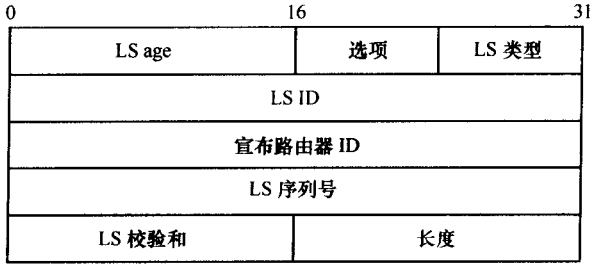

图 1.3　LSA 头格式

LS 序列号为 32bit，用来指示该 LSA 的更新程度。LS 序列号是一个有符号整型数，大小介于 0x80000001（负值）和 0x7fffffff 之间。较大的 LSA 序列号表示该 LSA 已经被更新。值得注意的是，任何一个路由器都可以更改这个 LSA 的头信息。一个攻击者收到一个 LSA 之后，可以把 LS 序列号加 1（Seq++攻击），它只要重新计算 LS 校验和保证该 LSA 有效，然后把这个 LSA 再次散发给其他路由器，其他路由器收到该 LSA 发现 LS 序列号已经加 1，这意味着 LSA 已经被更新，它就更新自己的路由状态，并继续散发该 LSA，一直到该 LSA 的创建者收到这个 LSA，发现 LSA 的内容不对头，它就重新发出一个新的 LSA 给其他路由器。如果攻击者不停地修改收到的 LSA 的序列号，那么造成的结果是整个网络运行不稳定。

除了把序列号加 1，攻击者还可以把序列号改成最大值，即 0x7fffffff（MaxSeq 攻击）。当然，每次修改 LSA，攻击者都要重新计算校验和以保证 LSA 是有效的。当该 LSA 到达自己的创建者，它就被重新设置并再次传播。如果攻击者不停地修改收到的 LSA 的序列号，同样也会造成整个网络运行不稳定。

OSPF 的第三种攻击方法就是 MaxAge 攻击。当攻击者收到一个 LSA，它把该 LSA 的 age 项设成最大值（一般是 3600），然后传给其他路由器。其他路由器收到该 LSA 以后，就把该 LSA 在自己路由状态中的信息清除。当该 LSA 的创建者收到它以后，该 LSA 再次被重新设置，并再次传播。和上面的攻击一样，这种攻击也会造成整个网络运行不稳定。

5．BGP 缺陷

BGP（Border Gateway Protocol）是自治域（AS）的核心路由器之间的路由信息交换协议。和 TCP/IP 协议一样，BGP 也包含着多种安全隐患，如 IP 欺骗、窃听、SYN 攻击等。任何一个实体可以在一个 BGP 的连接中加入信息或者中断这个连接。再加上 IP 欺骗的攻击技术，一个实体可以远程重置世界上任何 BGP 路由器。

BGP 之所以隐含着这么多安全问题是因为，它没有一个保护 BGP 连接消息的完整性、有效性和身份认证的机制。另外，没有一个确认 NLRI（Network Layer Reachability Information）

和 AS_PATH 项的有效性。

BGP 有四种消息类型：OPEN、KEEPALIVE、NOTIFICATION 和 UPDATE。任何一个实体都可以伪造 OPEN、KEEPALIVE 和 NOTIFICATION 消息去破坏一个 BGP 的连接。它还可以伪造 UPDATE 消息中的 ATOMIC_AGGREGATE、AS_PATH 或者 NLRI 项去破坏路由功能。在运行 BGP 协议的路由器出现问题后，所引起的后果将是灾难性的，这有可能会导致整个 ISP 网络无法访问，因此，这样的安全攻击更为严重。幸运的是，通常大多数核心路由器都已经做了严格的访问权限控制，入侵者能够直接攻击核心路由器的可能性并不是很大。

目前已经有一些针对 BGP 的安全扩展，例如对 BGP 报文加入完整性校验选项，从而避免这种风险，不过，大多数的 ISP 还是更喜欢用访问权限控制来解决这个问题，因为这样带来的影响要小得多。

1.1.3 监听（Sniff）、假冒（Spoof）和劫持（Hijack）

我们知道，IP 数据包一般是明文传输，而且也没有对来源的验证。这两个问题，就成了 TCP/IP 网络中最严重的安全隐患之一。内容不进行加密，使得在广播型的局域网络中，数据很容易被窃听。例如，在以太网中，只要将网卡设置为混杂模式，就可以监听到所有的数据包。通过对这些数据包的分析，攻击者可能从中取得必要的认证信息或重要的内容，例如，应用协议如 Telnet、FTP、POP3 等密码都是明文传输，如果这些密码在网上传输的时候被攻击者监听到，就会造成很大的安全隐患。或者，数据中含有个人敏感信息、商业机密等，如果被监听也会造成重大的损失。即使监听看不到数据的具体内容，也可以从中分析出哪些主机开了哪些服务，哪些主机和哪些主机之间进行了通信，从而可以分析出主机之间的信任关系。这些信息都会造成安全问题。

缺乏源认证是另外一个重要的问题。攻击者可以伪装成其他用户，从而取得不应有的特权，例如，攻击者通过伪造其他 IP 地址进行流量盗用。此外，如果攻击者使用其他 IP 地址进行恶意攻击，可以有效地隐藏自己的来源，同时给被假冒者名誉、性能等众多方面造成损害。伪造 ARP 就是一种常见的 IP 地址假冒方法，它的主要原理是，以被假冒主机的 IP 地址和本机的以太网地址为源地址发 ARP 包，这样即可造成 IP 地址的假冒。使用 IP 包头中的源路由选项是进行 IP 地址假冒的另外一种方法，通过指定 IP 包的源路由选项，一个 IP 包可以按照预先指定的路由到达目的主机，因为在一般情况下，一端使用源路由选项常常表示这一端有充足理由（如拥塞避免、故障路由的回避，以及效率方面的考虑）认定源路由有更好的表现，那么，很有可能目的主机使用该源路由的逆向路由与源主机通信，这样就实现了源 IP 的假冒。

攻击者甚至可以劫持一个连接，而让自己成为其中的中介。这也就是说，攻击者在某种意义上就像两个会话主体的中间人一样，进行互相转发。攻击者可以在其中增加、删除一些会话内容，而会话的双方对此完全不知情。这样的话，双方的通信就毫无安全可言了。一般而言，只要攻击者能够成功地假冒为其中一方，就能够进行会话的劫持。

综合利用其他一些协议的安全问题，即使在非广播的局域网或者广域网中，这种监听、假冒、劫持的风险仍然存在。

1. TCP 序列号预测

TCP 序列号预计由莫里斯首次提出，是网络安全领域中最有名的缺陷之一。这种攻击的

实质，是在不能接到目的主机应答确认包时通过预计序列号来建立连接。这样，入侵者可以伪装成信任主机与目的主机通话。

正常的 TCP 连接建立过程是一个三次握手的过程，客户方取一初始序列号 ISN_C 并发出第一个 SYN 包，服务方确认这一包并设自己一方的初始序列号为 ISN_S，客户方确认后这一连接即建立。一旦连接建立成功，客户方和服务方之间可以开始传输数据。连接建立过程可以被描述如下：

TCP 连接建立过程

客户方 → 服务方：SYN（ISN_C）

服务方 → 客户方：ACK（ISN_C），SYN（ISN_S）

客户方 → 服务方：ACK（ISN_S）

客户方 → 服务方：数据

和/或者

服务方 → 客户方：数据

由此可见，在连接建立的过程中，客户方必须收到来自服务方的初始序列号 ISN_S，在接收到 ISN_S 之前，对客户方来说它是一个随机数。

假设，入侵者通过某种方法得到了服务方的初始序列号 ISN_S，那么，它有可能冒充为另一个信任主机对目的主机发信息。这个过程如下：

攻击者 → 服务方　　：SYN（ISN_X），SRC = 被冒充的主机

服务方 → 被冒充的主机　：ACK（ISN_X），SYN（ISN_S）

攻击者 → 服务方　　：ACK（ISN_S），SRC = 被冒充的主机

攻击者 → 服务方　　：ACK（ISN_S），SRC = 被冒充的主机，数据

（其中，ISN_X 是来自攻击者的初始序列号）

由此可见，攻击者可以向服务方发送任意数据。如果此连接允许远程执行命令（例如 rsh），那么攻击者可以在服务方执行任何操作。

在这种入侵方法中，ISN_S 的预测是一个核心问题，所以这种缺陷依赖于 TCP 序列号的可预测性。ISN_S 是由操作系统所实现的 TCP/IP 模块产生的。对于不同操作系统，TCP/IP 模块的实现也不同，所以 ISN_S 产生的机制也有所不同。在老的 Berkeley 系统中，初始序列数变量每隔一秒都被增加一个固定值，连接被初始化以后，这个固定值减一半。因此，如果攻击者向服务方建立一个正常的连接并根据观察到来自服务方的初始序列号 ISN_S，他就能够比较准确地预测出在任意时刻该服务方上的初始序列数变量的值，也就是说可以预测出 ISN_S。TCP 序列号攻击的另一个变种就是利用 netstat 服务。如果目标主机上运行 netstat 服务，它会提供该主机上其他端口的 TCP 序列号的信息。在这种情况，攻击者不用预测而直接得到 ISN_S。目前的一些新的操作系统，ISN 的产生也并不是完全随机的，例如，一些操作系统所产生的值是递增的，还有一些操作系统所产生的值，虽然表面上看是随机的，但是仔细分析可能会发现它们的分布并不是均匀分布，而是可能会有一些像吸引子（Strange Attractor）之类的东西。

实际上，在以上的传输过程中，从服务方发送到被冒充的主机。

服务方→被冒充的主机：ACK（ISN_X），SYN（ISN_S）

有可能会被被冒充的那个主机收到，这时候它会发现这是一个不存在的连接，它就发送一个 RST 包阻止连接的建立。为了克服这个问题，攻击者可以向被冒充的主机发送大量 SYN