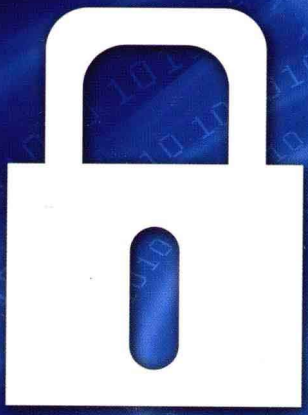

网络安全

新型技术研究及其应用

李洪伟◎著

电子科技大学出版社

网络安全

新型技术研究及其应用

WANGLUO ANQUAN

XINXING JISHU YANJIU JIQI YINGYONG

李洪伟◎著

电子科技大学出版社

图书在版编目（CIP）数据

网络安全新型技术研究及其应用 / 李洪伟著. —成都：电子科技大学出版社, 2011.3

ISBN 978-7-5647-0783-5

Ⅰ. ①网… Ⅱ. ①李… Ⅲ ①计算机网络－安全技术 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2011）第 028265 号

网络安全新型技术研究及其应用

李洪伟 著

出　　版：电子科技大学出版社（成都市一环路东一段 159 号电子信息产业大厦　邮编：610051）

策划编辑：梁瓔婕

责任编辑：李小锐

主　　页：www.uestcp.com.cn

电子邮箱：uestcp@uestcp.com.cn

发　　行：新华书店经销

印　　刷：成都市新都华兴印务有限公司

成品尺寸：140mm×203mm　印张 7.125　字数 205 千字

版　　次：2011 年 3 月第一版

印　　次：2011 年 3 月第一次印刷

书　　号：ISBN 978-7-5647-0783-5

定　　价：16.00 元

前　言

公钥密码系统面临的挑战不仅包括寻找和实现安全算法，还包括建立支持公钥认证的基础设施。在传统的公钥基础设施 PKI 中，证书用来保证公钥和身份之间的联系，实现公钥的认证。但是，PKI 在实践中面临很多挑战，例如可扩展性和证书的管理。为了解决 PKI 的这些问题，Shamir 在 1985 年提出了基于身份的密码体制（IBC）。在 IBC 中，公钥直接从用户唯一可标识的身份信息中获得，例如用户的姓名或者 Email 地址等，公钥的认证不再需要证书。IBC 是解决公钥认证的另外一种有效方法，和传统 PKI 相比，IBC 在密钥管理上有很大的优势。Shamir 在提出 IBC 概念的同时构造了第一个基于身份的签名方案，但是在基于身份加密方面的研究工作一直都没有多大的进展。直到 2001 年，Boneh 与 Franklin 首次利用 Weil 对提出了一个实用安全的基于身份加密方案，使基于身份的公钥密码重新成为一个研究热点，许多基于身份的密码系统相继提出。然而，在 IBC 中还存在一些有待解决的公开问题，如密钥托管、密钥撤销、密钥进化、安全模型等问题。研究和解决这些问题对 IBC 无论在理论上还是实践中都具有重要的意义。本书针对 IBC 中存在的问题进行了深入的研究，提出了一些有效的解决方案，取到了一些研究成果。本书的主要研究工作如下：

1．研究了基于身份的认证协议。提出了一种基于身份的无线局域网认证协议，并阐述了协议实现的硬件环境和流程。

2．提出了一个改进的基于身份的加密算法 IIBE。该算法的设计思想介于传统公钥加密和基于身份的公钥加密之间。与传统的

公钥加密相比，该算法不需要公钥证书，免去了对证书的管理；与基于身份的公钥加密相比，该算法解决了密钥托管和密钥撤销问题。IIBE 用椭圆曲线上的双线性映射构造，其安全性基于 Bilinear Diffie-Hellman 问题的计算困难性假设。在 Random Oracle 下，该算法具有自适应选择密文的语义安全性。

3．研究了基于身份的密钥进化算法。首先提出了基于身份的前向安全加密算法 IBE-FS，该算法中，第 t 时间周期的密钥泄漏，第 $t'(t'<t)$ 时间周期的密钥依然安全，并证明了算法的安全性，在仿真实验中分析了算法的性能。进一步提出了一个基于身份的抗入侵加密算法 IBE-IR，该算法在前向安全的基础上，增加一个帮助设备，密钥的进化由帮助设备和用户共同完成，实现了密钥的前向安全性和后向安全性，在帮助设备密钥泄漏的前提下，依然保证密钥的前向安全性。与 Dodis 方案比较，在取得相同密钥安全性的情况下，部分算法计算复杂度却降低到 $O(1)$。仿真实验表明，IBE-IR 比 Dodis 方案更高效。

4．在网格环境中研究基于身份的密码算法。首先提出了基于身份的网格体系结构 IBAG，该结构不需要数字证书。接着给出了 IBAG 中基于身份的加密算法 IBE 和签名算法 IBS，证明了 IBE 的安全性，通过仿真实验分析了 IBE 和 IBS 的性能。然后提出了 IBAG 中基于身份的认证协议 IBAP，该协议以基于身份的网格体系结构为基础，嵌入了 IBE 与 IBS。仿真实验表明，IBAP 比 SAP 更轻量、更高效，特别是用户端的负担大大减轻，有助于网格规模的扩大。最后提出了一种 GSI 的改进方案，该方案对 GSI 的 3 组协议进行了改进。仿真实验表明，改进方案比 GSI 更高效。

编者

2011 年 2 月

目　录

第 1 章　网络安全风险分析

1.1　TCP/IP 协议缺陷

1.1.1　TCP/IP 概述

TCP/IP 指传输控制协议/网际协议（Transmission Control Protocol/Internet Protocol）。TCP/IP 定义了电子设备（比如计算机）如何连入因特网，以及数据如何在它们之间传输的标准。TCP/IP（传输控制协议/网际协议）是互联网中的基本通信语言或协议。在私网中，它也被用作通信协议。当你直接网络连接时，你的计算机应提供一个 TCP/IP 程序的副本，此时接收你所发送的信息的计算机也应有一个 TCP/IP 程序的副本。

TCP/IP 是一个四层的分层体系结构。高层为传输控制协议，它负责聚集信息或把文件拆分成更小的包。这些包通过网络传送到接收端的 TCP 层，接收端的 TCP 层把包还原为原始文件。低层是网际协议，它处理每个包的地址部分，使这些包正确的到达目的地。网络上的网关计算机根据信息的地址来进行路由选择。即使来自同一文件的分包路由也有可能不同，但最后会在目的地汇合。TCP/IP 使用客户端/服务器模式进行通信。TCP/IP 通信是点对点的，意思是通信是网络中的一台主机与另一台主机之间的。TCP/IP 与上层应用程序之间可以说是“没有国籍”，因为每个客户请求都被看做是与上一个请求无关的。正是它们之间的“无国籍”释放了网络路径，才使每个人都可以连续不断的使用网络。

许多用户熟悉使用 TCP/IP 协议的高层应用协议。包括万维网的超文本传输协议（HTTP），文件传输协议（FTP），远程网络访问协议（Telnet）和简单邮件传输协议（SMTP）。这些协议通常和 TCP/IP 协议打包在一起。使用模拟电话调制解调器连接网络的个人电脑通常是使用串行线路接口协议（SLIP）和点对点协议（P2P）。这些协议压缩 IP 包后通过拨号电话线发送到对方的调制解调器中。与 TCP/IP 协议相关的协议还包括用户数据包协议（UDP），它代替 TCP/IP 协议来达到特殊的目的。其他协议是网络主机用来交换路由信息的，包括 Internet 控制信息协议（ICMP）、内部网关协议（IGP）、外部网关协议（EGP）和边界网关协议（BGP）。

1.1.2 TCP/IP 整体构架

TCP/IP 协议并不完全符合 OSI 的七层参考模型。传统的开放式系统互联参考模型，是一种通信协议的七层抽象的参考模型，其中每一层执行某一特定任务。该模型的目的是使各种硬件在相同的层次上相互通信。这七层是：物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。而 TCP/IP 通信协议采用了四层的层级结构，每一层都呼叫它的下一层所提供的网络来完成自己的需求。如图 1-1 所示这四层分别为：

应用层：应用程序间沟通的层，如简单电子邮件传输（SMTP）、文件传输协议（FTP）、网络远程访问协议（Telnet）等。

传输层：在此层中，它提供了节点间的数据传送，应用程序之间的通信服务，主要功能是数据格式化、数据确认和丢失重传等。如传输控制协议（TCP）、用户数据报协议（UDP）等，TCP 和 UDP 给数据包加入传输数据并把它传输到下一层中，这一层负责传送数据，并且确定数据已被送达并接收。

互联网络层：负责提供基本的数据封包传送功能，让每一块数据包都能够到达目的主机（但不检查是否被正确接收），如网际

协议（IP）。

网络接口层（主机—网络层）：接收 IP 数据包并进行传输，从网络上接收物理帧，抽取 IP 数据包转交给下一层，对实际的网络媒体的管理，定义如何使用实际网络（如 Ethernet、Serial Line 等）来传送数据。

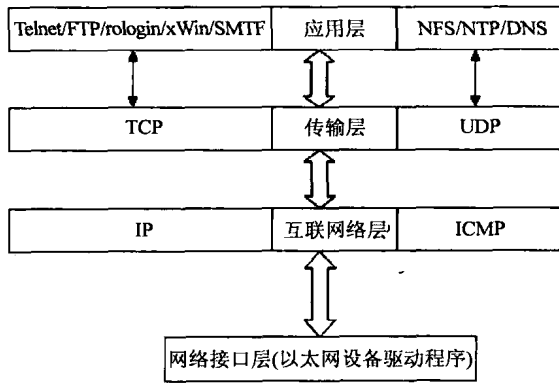

图 1-1　TCP/IP 协议结构图

以下简单介绍 TCP/IP 中的协议都具备什么样的功能，都是如何工作的。

1．IP

网际协议 IP 是 TCP/IP 的心脏，也是网络层中最重要的协议。IP 层接收由更低层（网络接口层，例如以太网设备驱动程序）发来的数据包，并把该数据包发送到更高层——TCP 或 UDP 层；相反，IP 层也把从 TCP 或 UDP 层接收来的数据包传送到更低层。IP 数据包是不可靠的，因为 IP 并没有做任何事情来确认数据包是按顺序发送的或者没有被破坏。IP 数据包中含有发送它的主机的地址（源地址）和接收它的主机的地址（目的地址）。

高层的 TCP 和 UDP 服务在接收数据包时，通常假设包中的

源地址是有效的。也可以这样说，IP 地址形成了许多服务的认证基础，这些服务相信数据包是从一个有效的主机发送来的。IP 确认包含一个选项，叫做 IP source routing，可以用来指定一条源地址和目的地址之间的直接路径。对于一些 TCP 和 UDP 的服务来说，使用了该选项的 IP 包好像是从路径上的最后一个系统传递过来的，而不是来自于它的真实地点。这个选项是为了测试而存在的，说明了它可以被用来欺骗系统来进行平常是被禁止的连接。那么，许多依靠 IP 源地址做确认的服务将产生问题并且会被非法入侵。

2．TCP

如果 IP 数据包中有已经封好的 TCP 数据包，那么 IP 将把它们向“上”传送到 TCP 层。TCP 将包排序并进行错误检查，同时实现虚电路间的连接。TCP 数据包中包括序号和确认，所以未按照顺序收到的包可以被排序，而损坏的包可以被重传。

TCP 将它的信息送到更高层的应用程序，例如 Telnet 的服务程序和客户程序。应用程序轮流将信息送回 TCP 层，TCP 层便将它们向下传送到 IP 层，设备驱动程序和物理介质，最后到接收方。

面向连接的服务（例如 Telnet、FTP、rlogin、X Windows 和 SMTP）需要高度的可靠性，所以它们使用了 TCP。DNS 在某些情况下使用 TCP（发送和接收域名数据库），但使用 UDP 传送有关单个主机的信息。

3．UDP

UDP 与 TCP 位于同一层，但它不管数据包的顺序、错误或重发。因此，UDP 不被应用于那些使用虚电路的面向连接的服务，UDP 主要用于那些面向查询——应答的服务，例如 NFS。相对于 FTP 或 Telnet，这些服务需要交换的信息量较小。使用 UDP 的服务包括 NTP（网络时间协议）和 DNS（DNS 也使用 TCP）。

欺骗 UDP 包比欺骗 TCP 包更容易，因为 UDP 没有建立初始

化连接（也可以称为握手），在两个系统间也没有虚电路，也就是说，与 UDP 相关的服务面临着更大的危险。

4．ICMP

ICMP 与 IP 位于同一层，它被用来传送 IP 的控制信息。它主要是用来提供有关通向目的地址的路径信息。ICMP 的“Redirect”信息通知主机通向其他系统的更准确的路径，而“Unreachable”信息则指出路径有问题。另外，如果路径不可用了，ICMP 可以使 TCP 连接“体面地”终止。PING 是最常用的基于 ICMP 的服务。

5．TCP 和 UDP 的端口结构

TCP 和 UDP 服务通常有一个客户/服务器的关系，例如，一个 Telnet 服务进程开始在系统上处于空闲状态，等待着连接。用户使用 Telnet 客户程序与服务进程建立一个连接。客户程序向服务进程写入信息，服务进程读出信息并发出响应，客户程序读出响应并向用户报告。因而，这个连接是双工的，可以用来进行读写。

两个系统间的多重 Telnet 连接是如何相互确认并协调一致呢？TCP 或 UDP 连接唯一地使用每个信息中的如下四项进行确认：源 IP 地址发送包的 IP 地址；目的 IP 地址接收包的 IP 地址；源端口源系统上的连接的端口；目的端口目的系统上的连接的端口。

端口是一个软件结构，被客户程序或服务进程用来发送和接收信息。一个端口对应一个 16 bit 的数。服务进程通常使用一个固定的端口，例如，SMTP 使用 25、Xwindows 使用 6000。这些端口号是“广为人知”的，因为在建立与特定的主机或服务的连接时，需要这些地址和目的地址进行通讯。

1.1.3 TCP/IP 协议簇、参考模型、IP 地址及其分类

TCP/IP（Transmission Control Protocol/Internet Protocol）已成为一个事实上的工业标准。TCP/IP 是一组协议的代名词，它还包括许多协议，组成了 TCP/IP 协议簇。 TCP/IP 协议簇分为四层，

IP 位于协议簇的第二层（对应 OSI 的第三层），TCP 位于协议簇的第三层（对应 OSI 的第四层）。

在 Internet 上连接的所有计算机，从大型机到微型计算机都是以独立的身份出现，我们称它为主机。为了实现各主机间的通信，每台主机都必须有一个唯一的网络地址。就好像每一个住宅都有唯一的门牌一样，才不至于在传输资料时出现混乱。

Internet 的网络地址是指连入 Internet 网络的计算机的地址编号。所以，在 Internet 网络中，网络地址唯一地标识一台计算机。Internet 是由几千万台计算机互相连接而成的。而我们要确认网络上的每一台计算机，靠的就是能唯一标识该计算机的网络地址，这个地址就叫做 IP（Internet Protocol）地址，即用 Internet 协议语言表示的地址。

目前，在 Internet 里，IP 地址是一个 32 位的二进制地址，为了便于记忆，将它们分为 4 组，每组 8 位，由小数点分开，用四个字节来表示，而且，用点分开的每个字节的数值范围是 0~255，如 202.116.0.1，这种书写方法叫做点数表示法。

IP 地址可确认网络中的任何一个网络和计算机，而要识别其他网络或其中的计算机，则是根据这些 IP 地址的分类来确定的。一般将 IP 地址按节点计算机所在网络规模的大小分为 A、B、C 三类，默认的网络屏蔽是根据 IP 地址中的第一个字段确定的。

1．一个 A 类 IP 地址由 1 字节（每个字节是 8 位）的网络地址和 3 个字节主机地址组成，网络地址的最高位必须是“0”，即第一段数字范围为 1～127。每个 A 类地址理论上可连接 16777214<256*256*256–2>台主机（–2 是因为主机中要用去一个网络号和一个广播号），Internet 有 126 个可用的 A 类地址。A 类地址适用于有大量主机的大型网络。

2．B 类地址的表示范围为：128.0.0.1~191.255.255.255，默认网络屏蔽为：255.255.0.0；B 类地址分配给一般的中型网络。B 类

网络用第一、二组数字表示网络的地址，后面两组数字代表网络上的主机地址。

3．C 类地址的表示范围为：192.0.0.1~223.255.255.255，默认网络屏蔽为：255.255.255.0；C 类地址分配给小型网络，如一般的局域网，它可连接的主机数量是最少的，采用把所属的用户分为若干的网段进行管理。C 类网络用前三组数字表示网络的地址，最后一组数字作为网络上的主机地址。

4．D 类地址不分网络地址和主机地址，它的第 1 个字节的前四位固定为 1110。D 类地址范围：224.0.0.1 到 239.255.255.254 。D 类地址用于多点播送。D 类地址称为广播地址，供特殊协议向选定的节点发送信息时用。

5．E 类地址保留给将来使用。

1.1.4 TCP/IP 攻击

由于 TCP/IP 协议是 Internet 的基础协议，所以对 TCP/IP 协议的完善和改进是非常必要的。TCP/IP 协议从开始设计时并没有考虑到现在网络上如此多的威胁，由此导致了许多形形色色的攻击方法，一般针对协议原理的攻击（尤其是 DDOS），我们无能为力。

1．TCP/IP 攻击的常用原理

（1）源地址欺骗（Source Address Spoofing）、IP 欺骗（IP Spoofing）和 DNS 欺骗（DNS Spoofing）。其基本原理是：利用 IP 地址并不是出厂的时候与 MAC 固定在一起，攻击者通过自封包和修改网络节点的 IP 地址，冒充某个可信节点的 IP 地址进行攻击。主要有三种手法：瘫痪真正拥有 IP 的可信主机；伪装可信主机攻击服务器；中间人攻击；DNS 欺骗（DNS Spoofing）和“会话劫持”（Session Hijack）。

（2）源路由选择欺骗（Source Routing Spoofing）。原理：利用 IP 数据包中的一个选项——IP Source Routing 来指定路由，利

用可信用户对服务器进行攻击，特别是基于 UDP 协议的，由于其是面向非连接的，更容易被利用来攻击。

（3）路由选择信息协议攻击（RIP Attacks）。原理：攻击者在网上发布假的路由信息，再通过 ICMP 重定向来欺骗服务器路由器和主机，将正常的路由器标志为失效，从而达到攻击的目的。

（4）TCP 序列号欺骗和攻击（TCP Sequence Number Spoofing and Attack），基本有三种： 伪造 TCP 序列号，构造一个伪装的 TCP 封包，对网络上可信主机进行攻击；SYN 攻击（SYN Attack）。这类攻击手法花样很多，蔚为大观。但是其原理基本一致，让 TCP 协议无法完成三次握手协议；Teardrop 攻击（Teardrop Attack）和 Land 攻击（Land Attack）。原理：利用系统接收 IP 数据包，对数据包长度和偏移不严格的漏洞进行攻击。

2．IP 攻击方式

（1）OOB 攻击：这是利用 NETBIOS 中一个 OOB（Out of Band）的漏洞而进行的，它的原理是通过 TCP/IP 协议传递一个数据包到计算机某个开放的端口上（一般是 137、138 和 139），当计算机收到这个数据包之后就会瞬间死机或者蓝屏现象，不重新启动计算机就无法继续使用 TCP/IP 协议来访问网络。

（2）DOS 攻击：这是针对 Windows 9X 所使用的 ICMP 协议进行的 DOS（Denial of Service，拒绝服务）攻击，一般来说，这种攻击是利用对方计算机上所安装协议的漏洞来连续发送大量的数据包，造成对方死机。

（3）WinNuke 攻击：目前的 WinNuke 系列工具已经从最初的简单选择 IP 攻击某个端口发展到可以攻击一个 IP 区间范围的计算机，并且可以进行连续攻击，还能够验证攻击的效果，以及可以检测和选择端口，因此使用它可以造成某一个 IP 地址区间的计算机全部蓝屏死机。

（4）SSPing：这是一个 IP 攻击工具，它的工作原理是向对

方的计算机连续发出大型的 ICMP 数据包，被攻击的计算机此时会试图将这些文件包合并处理，从而造成系统死机。

（5）TearDrop 攻击：这种攻击方式利用那些在 TCP/IP 堆栈实现中信任 IP 碎片中的包的标题头所包含的信息来实现自己的攻击，由于 IP 分段中含有指示该分段所包含的是原包哪一段的信息，所以一些操作系统下的 TCP/IP 协议在收到含有重叠偏移的伪造分段时将崩溃。TearDrop 最大的特点是除了能够对 Windows 9X/NT 进行攻击之外，连 Linux 也不能幸免。

利用协议实现的攻击方法，都是故意错误地设定数据包头的一些重要字段，例如，IP 包头部的 Length、Fragment offset、IHL 和 Source address 等字段。使用 Raw Socket 将这些错误的 IP 数据包发送出去。在接收数据端，接收程序时通常都存在一些问题，因而在将接受到的数据包组装成一个完整的数据包的过程中，就会使系统当机、挂起或系统崩溃。

3．攻击的现象及其后果

使用了 Windows 95 和 Windows 98 NT 的人们都经历过系统陷入混乱，对任何输入都没有响应的情况：屏幕出现蓝屏，迟迟无法重新刷新。按下 Ctrl+Alt+Del 时，看到系统 CPU 利用率达到 100%，同时显示一个应用程序无响应。这是程序出错或者使用了盗版软件的缘故。通过网络，也可以使正在使用的计算机出现这种无响应、死机的现象。事实上，大量的程序往往经不住人们恶意的攻击。

人们已经使用了许多方法来专门对付上网的 Windows 95 和 Windows NT。目前，能够对 Windows 95 和 Windows NT 进行攻击的方法很多，当前流行的有：TearDrop（也称为“泪滴”）、OOB、Land、Ping of Death 等。其中，关于 Ping of Death 在缓冲区溢出一章中对这种攻击做了介绍，并给出了一些对策。一般的攻击过程是这样的：当入侵者发现了一台 Windows 95 或者 Windows NT

（这只需用端口扫描工具扫一下就可以辨认出来），便用一个OOB 或者 TearDrop 攻击，再次用 ping 命令时，目标主机就没有响应了。事实上，这些攻击并不是局限于 Windows NT 和 Windows 95 平台，一些攻击，如 Land 已被发现对 Linux、Cisco 路由器以及其他大量的 UNIX 操作系统都具有相当的攻击能力。

能够实施这种攻击的原因是在 Windows 95 和 Windows NT 中存在错误，这是一种处理 TCP/IP 协议或者服务程序的错误。人们利用这些错误。通过给端口发送一些故意弄错的数据包，在这个数据包的偏移字段和长度字 6 段，写入一个过大或过小的值，Windows 95 和 Windows NT 都不能处理这个情况，然后 Windows 95 就先变成蓝屏，Windows NT 是非死机不可。据称 TearDrop 可以使被攻击的主机立刻当机。这些攻击的危险性在于可以通过网络发起攻击，当攻击者发现了一台上网的 Windows 95、Windows NT 或者 Linux 操作系统主机时，只需启动这一程序，输入入口参数假冒 IP、端口号，被攻击主机的 IP 地址和端口号，便可以发起攻击了。通常是 Linux 遭到攻击就当机，而 Windows 在受到十几次攻击之后也会死机。这时候，用 ping 命令，被攻击的主机就再也没有回应了。服务程序存在错误的情况是很多的，例如，Windows NT 中的 RPC 服务存在漏洞。某个用户可以远程登录到 Windows NT 3.5x 或者服务器的端口 135，并任意输入 10 个字符，然后回车，切断连接，这便可以使目标主机的 CPU 利用率达到 100%。虽然一个简单的重启动就消除了这个问题，但毕竟这是很讨厌的，是系统安全的重要隐患并严重地影响系统性能。

对于 OOB 攻击，人们已经提出一些对策，如在 Windows NT 4.0 中，对发到端口 39 的包进行过滤等，都需要对系统的网络设置进行一番配置，来分别处理拨号上网和使用 LAN 的情况。目前网上已经出现补丁程序，用来对付这些攻击方法的攻击。在 Windows 95 和 Windows NT 上的安装非常简单，只需运行一下安装包即可。