主流即时通软件通信协议分析*

李远杰[1]，刘渭锋[1,2]，张玉清[2]，梁　力[1]

(1. 西安交通大学 计算机科学与技术系，陕西 西安 710049；2. 中国科学院 研究生院 国家计算机网络入侵防范中心，北京 100039)

摘　要: 根据主流即时通软件通信数据明文传输的特点,利用网络捕包工具,采用逆推的方法,分析目前流行的即时通软件不公开且不统一的文本消息传输协议。着重描述了 ICQ 文本消息传输协议的格式,并且对 ICQ、AIM、MSN、雅虎通几个主流即时通软件的协议特征进行了比较说明,为进一步的文本消息监控提供依据。

关键词: 即时通；协议分析；嗅探

中图法分类号: TP393.04　　**文献标识码**: A　　**文章编号**: 1001-3695(2005)07-0243-03

Analysis of Text Message Transmitting Protocol in Popular Instant Messenger Software

LI Yuan-jie[1], LIU Wei-feng[1,2], ZHANG Yu-qing[2], LIANG Li[1]

(1. Dept. of Computer Science & Technology, Xi'an Jiaotong University, Xi'an Shanxi 710049, China; 2. National Computer Network Intrusion Protection Center, Graduate School, Chinese Academy of Sciences, Beijing 100039, China)

Abstract: Based on the exoteric communication data between popular instant messenger client software, using sniffer tool of network, we analyse the unopened and nonuniform text message transmitting protocol of those software by converse way. Particularly describe the form of ICQ text message transmitting protocol and compare the characteristic of ICQ, AIM, MSN and Yahoo Messgeger protocol. Provide reference for text message transmitting monitor in the future.

Key words: Instant Messenger(IM); Protocol Analysis; Sniffer

在当今信息时代,人们之间的信息交流需求越来越高,即时通(Instant Messenger, IM)软件应运而生,立即受到广大互联网用户的喜爱,风靡全球。在我国流行的 IM 软件品种繁多,有国内腾讯公司的 QQ,国外的 ICQ, AIM, MSN 和 Yahoo Messenger 等即时通产品。其中 ICQ 和 AIM 是美国在线公司 AOL 出品的两款流行的即时通软件,ICQ 凭借它推出时间最长和强大的功能依然占据着即时通主流的位置。目前最新版本是 ICQPro2003a, AIM 是 5.2 版本。MSN 是微软推出的即时通产品,它最大的特点就是将个人邮箱与即时通信功能完善结合。目前最新中文版本是 MSN 6.0 版。Yahoo Messenger 中文名字叫雅虎通,由世界著名搜索引擎 Yahoo 推出,它的最新简体中文版本是 5.5 版。这些主流的即时通软件拥有绝大部分的用户群,而且随着功能的完善,服务的加强,对人们生活的影响将越来越大,因此对即时通软件的监控和通信协议分析变得越来越重要。这些主流即时通软件的协议格式各不相同,由于即时通软件公司出于自身利益的考虑,各自保守着各自的协议格式和相关通信技术,通过提供特色的服务,来吸引各自的用户群。这种协议的不统一性和不公开性,严重束缚着即时通软件快速发展,也束缚着对这些软件的监控。因此对这些主流即时通通信软件协议格式的分析意义重大。

收稿日期: 2004-07-01；修返日期: 2004-09-06

基金项目: 国家“863”计划资助项目(2003AA142150)；中国科学院知识创新工程方向性项目(KGCX2-106)；北京市科技计划项目(H020120090530)

1　协议分析的环境配置

为了便于逐一分析这些即时通软件的通信协议,区别同一子网的端与端通信和不同子网端与端通信协议格式的不同,我们搭建简单的分析实验平台,为协议的分析提供必要的硬件和软件支持。实验环境由四台 PC 机和一个集线器组成。其中两台 PC 机与集线器构成一个小型的内部局域网,通过一台作为网关的 PC 机连接到具有独立 IP 的大型局域网中(简称外网)。网关与另一台 PC 机都是外网的主机。配置如图 1 所示。

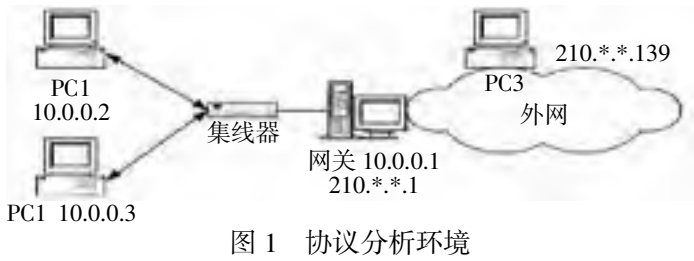

图 1　协议分析环境

网关采用双网卡配置,安装 Win 2000 Server 操作系统,利用 Server 操作系统自带的软件路由器实现路由功能。其他客户机均使用 Windows 操作系统。同时在所有的 PC 机上预安装 NAI 公司的 Snifferpro 4.7 试用版软件。

Sniffer 是捕获网络数据报文的一种工具,功能强大,使用方便。使用该工具时需要进行简单的设置,首先是确定将要抓取的数据包的协议类型,一般是基于 IP 协议的数据包;其次是数据包的源和目的端地址,地址一般分为硬件网卡地址和 IP

地址,通常选择 IP 地址,按照实验环境中分配的 IP 地址设置该条件;最后在客户端发送即时消息之前启动 Sniffer 工具的监听功能,它就能从大量的经过网关的数据包中提取出满足如上条件的数据包,为我们缩小了检索数据包的范围。

从捕获的数据包中可以利用 Sniffer 的协议分析功能取出应用层的数据,大部分主流即时通软件的应用层协议组织的数据在网路上明文传输,我们正是利用了这一点,通过实验环境中的客户端之间有目的地发送消息,比较应用层数据体中固定字节或者规律性字节的含义,总结出它们协议的格式。

利用如上的配置环境,通过网关上的 Sniffer 工具,我们可以轻松地抓取局域网内部客户端之间通信的数据包和局域网内部客户端与外网客户端的通信数据包的应用层数据,为我们下面协议分析做好了充分的准备。

2 ICQ 文本消息传输协议分析

选择 ICQ 通信协议的分析过程作为特例,有以下几点考虑:

(1) ICQ 是最早出现的即时通通信软件,具有代表性。

(2) ICQ 依然是目前主流的即时通软件。

(3) ICQ 协议是 AOL 公司将原 ICQ(1998 被 AOL 收购)和 AIM(AOL 自己的即时通产品)两大即时通软件的协议格式的综合。

(4) ICQ 应用层数据在网络上明文传输。

首先在各个试验环境的主机上安装 ICQ version 2003a 客户端,通过网上免费申请几个 ICQ 账号,并成功登录到服务器,客户端之间互相加盟为好友之后,即可进行消息通信。

2.1 ICQ 消息数据包的分析

消息数据包主要包括由客户端发送出去的数据包和客户端接收的数据包两种。在两个客户端反复地发送消息,在网关上抓取这些数据包并进行分析比较,即可对固定字段和有规律变化的字段有一个大概的认识。

图 2 是截获的一个应用层数据的分析示例,该数据是从客户端发送给服务器的消息数据。为了便于分析,将连续的二进制串用换行符分开,每行中的字节具有特定的意义(图 2)。同时根据各行字节之间的联系又将数据组织为层,每下一层总比上一层缩进两个字节的长度,如图 2 所示,可以看出我们总共划分了三层。

2a	节拍层首标
02	SNAC 通道
30 a4	节拍数据包的顺序号
01 a2	节拍的数据长度
00 04	客户端基本消息交互服务(ICMB)ID 号
00 06	发送通过服务器中转的消息的命令 ID 号
00 00	SNAC 标志位
00 02 00 06	会话 ID,服务器与客户端连接的标志
6e df 24 00 le 26 00 00	消息 ID 号,应答及从服务器返回该消息时使用数据类型
00 02	数据类型
09	用户 ID 号长度
33 30 31 35 34 34 32 36 36	用户 ID 号
00 05	ICMB 消息类型标志
01 7c	消息的长度
...	如上长度的消息数据,包括数据格式、编码方式、字体信息以及消息内容等

图 2 一个发送给服务器的应用层消息数据分析示例

在第三层中可以观察出数据是按照“数据类型、数据长度、数据体”的格式组织数据的,用英文表示就是“Type, Length, Value”,简称 TLV 格式。利用 TLV 格式组织数据非常方便和高效,尤其适用于可变长的数据。对于应用层数据体中内容的组织一般都是采用这种格式。对于节拍层,SNAC 通道等协议特定名词的解释在 2.2 中有详细说明。

2.2 ICQ 文本消息传输协议

ICQ 功能强大,因此协议非常庞大,在这里只介绍通过分析它的文本消息传输过程得到的协议,称它为文本消息传输协议。显然这个协议只是 ICQ 协议的一个子集,而对于即时通通信的监控正需要这部分协议。

ICQ 是通过 TCP 有连接服务上传送数据的,服务器端端口固定为 5190。在 TCP/IP 协议基础上,ICQ 文本消息传输的应用层又可分为两层,即节拍层和 SNAC 层。所谓节拍,就是 ICQ 客户端与服务器端之间的一次交互的数据包。SNAC 是建立在节拍层之上的一个数据通信层,它是客户端与服务器端交互的基本通信单元。对于节拍层通道位是 2 的情况,表明节拍层的下一层就是 SNAC 层。节拍层的协议格式如图 3 所示。

在节拍标志 2a 之后的一个字节是通道标志,通道根据节拍数据内容的不同被划分为五种,分别是:01 登录信息通道,02 SNACs 通道,03 出错信息通道,04 断开连接信息通道,05 是 PING 命令通道。

当客户端与服务器端通过通道 01 建立链接以后,用户消息只在通道 02 SNACs 上传输,只有当一个底层的节拍错误发生时,才使用通道。3 发送错误消息;当打算终止客户端与服务器之间的链接时才利用通道。4 进行协商。大部分在生命周期内的事件处理都是通过通道 02 进行的,因此文本消息只能通过 02 通道传输。当通道是 02 时,节拍层的数据部分对应的就是 SNAC 层。SNAC 层的协议格式如图 4 所示。

图 4 中,SNAC 层第一个双字节是家族标志,家族就是同一类型的服务的集合。ICQ 支持 9 种 SNAC 家族服务。家族 ID 和服务范围如表 1 所示。从表 1 的服务范围我们可以看出,与客户消息有关的服务一般都集中在 ICMB 家族服务中,ICMB 的家族标志是 0x0004,在这个家族中 ICMB 提供了 13 种子服务,这些服务对用户之间的基本信息交互功能进行了细分,不同的子功能承担着消息交互过程中不同的任务。在所有子服务中,与用户文本消息有关的子服务如表 2 所示。表 2 中,家族数组其实就是家族 ID 与家族子类型 ID 号的组合,这种组合可以具体定位一个数据包的具体功能。SNAC(0x04, 0x06)如图 2 示例中分析的那样,它是由客户端发出的经过服务器转发的消息包。SNAC(0x04, 0x07)则是发送给客户端的经由服务器转发的消息包。

2a 字节	节拍的 ID
xx 字节	节拍的通道
xx xx 双字节	节拍数据报的顺序号
xx xx 双字节	节拍的数据长度
	... 节拍数据

图 3 节拍层协议格式

xx xx 双字节	家族(服务)ID 号
xx xx 双字节	家族子服务 ID 号
xx xx 双字节	SNAC 标记位
xx xx xx xx 双字节(dword)	SNAC 请求 ID
	... SNAC 数据

图 4 SNAC 层协议格式

表 1 SNAC 家族服务表

家族 ID	服务范围格式
0x0001	一般服务控制
0x0002	本地服务
0x0003	好友列表管理服务
0x0004	客户端基本消息交互服务
0x0009	个人隐私管理服务
0x000f	用户的姓名地址录查询
0x0013	服务器端信息服务
0x0015	ICQ 特殊扩展服务
0x0017	授权/注册服务

表 2　ICMB 消息发送和接收服务表

ICMB 家族数组	家族子服务 ID 号	服务端	服务描述
SNAC(0x04, 0x06)	0x0006	客户端	客户端发送通过服务器的消息
SNAC(0x04, 0x07)	0x0007	服务器	发送给客户端的经过服务器的消息

利用以上的协议格式,我们就可以从所有的网络数据包中检索出用户的文本消息数据包,并通过对各个字段的分析,找到消息体。在 ICQ 中消息体是 RTF 格式的。RTF 是英文 Rich-Text Format 的缩写,即所谓的“富文本格式”,它比 Word 体积小,比 Text 容量大,是一种很通用的带格式文本文件格式。

通过以上分析, ICQ 的协议简洁明了,非常规整。协议按照分层结构组织数据,一般各层头部信息字段长度固定,格式比较稳定。对于数据体中变长的数据采用 TLV 格式组织,简单、高效,便于处理。协议的第一层是节拍层,该层的通道号是 02 时,确定了节拍层数据的内容对应的是 SNAC 层。在 SNAC 层中只需要简单地通过家族 ID 和家族子服务 ID 的组合是 SNAC(0x04, 0x06) 或者 SNAC(0x04, 0x07) ,就可以容易地断定该层数据体传输的是用户消息。

3　主流即时通软件的协议比较

在当今的主流即时通软件中, AIM、MSN、雅虎通都可以通过上述的方法进行分析。由于国内腾讯的 QQ 的应用层数据在网络传输时进行了加密,对它的协议进行分析,首先需要知道其加密/解密的算法,超出我们协议分析的范畴,因此在此没有列出。

3.1　即时通软件的通信架构

即时通系统一般有两种模式: 一个是用户/服务器模式,即发信端用户和收信端用户必须通过服务器来交流; 另一个是用户/用户模式,即服务器给每对用户建立一个 TCP 通道,他们的交流在这个 TCP 之上进行,无需通过服务器。上述主流软件使用的是用户/服务器的模式,文本消息必须通过服务器才能从一个用户端传送到另一个用户端。

这几个主流即时通软件的一般通信架构如图 5 所示。

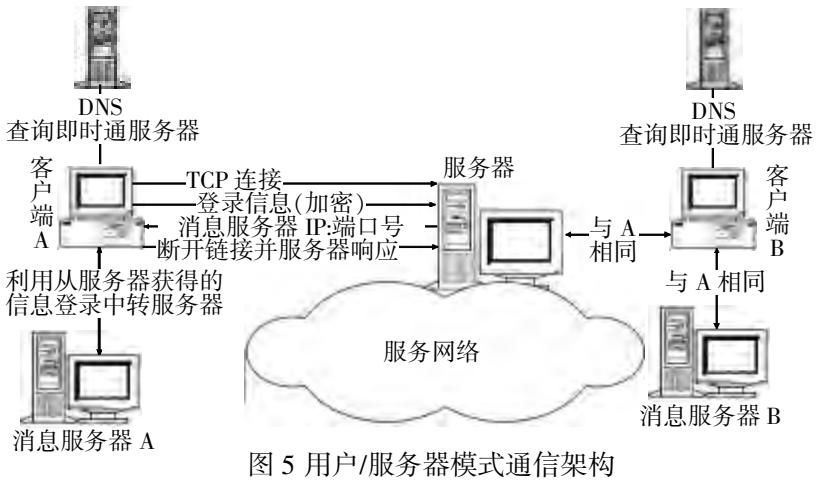

图 5 用户/服务器模式通信架构

对于文本消息的传送,除了通信架构都是基于客户端/服务器模式之外,消息传输都是建立在 TCP 协议基础之上的,而且服务器端的端口一般都是固定端口,服务器通过提供固定的服务端口被动式的与客户端进行通信,起到消息中转的作用。需要特殊说明的是,雅虎通对同一个局域网内的客户端通信采用用户/用户的通信架构。

3.2　主流即时通软件的文本消息协议特征比较

对表 3 需要进行以下说明:

(1) AIM 与 ICQ 同是 AOL 公司的产品,因此协议格式基本相同。有两点不同之处: 一是 AIM 支持聊天室消息发送和接收服务,分别如表 3 所示的 SNAC(0x0e, 0x05) 和 SNAC(0x0e, 0x06) 服务; 二是 AIM 采用 HTML 格式组织消息体数据。

(2) MSN 文本消息传输协议格式简单,应用层数据体以命令为首标,采用命令行的方式组织数据,命令使用 ASCII 码表示,统一采用三个字母组成,如“MSG”为消息传送命令,后面跟随零个或者更多个参数,参数之间被一个或者多个空格字符分开,命令结束通过回车换行符(CRLF) 表示。

表 3　四种 IM 文本消息传输协议特征对照表

种类 / 特征	ICQv2003a	AIM v5.2	MSN 6.0	雅虎通 5.5
服务端口	5190	5190	1863	5050
数据体首标	0x2a	0x2a	依据数据包命令不同,首标不定	0x594d5347(YMSG)
数据段组织方式	TLV	TLV	用回车换行符“0d0a”分隔数据段	用 0xc080 分隔数据段
发送消息标志	SNAC(0x04, 0x06)	SNAC(0x04, 0x06) 或 SNAC (0x0e, 0x05) (聊天室)	“MSG”命令标志	0x0006 或者 0x00a8) (聊天室)
接收消息标志	SNAC(0x04, 0x07)	SNAC(0x04, 0x07) 或 SNAC (0x0e, 0x06) (聊天室)	“MSG”命令标志	0x0006 或者 0x00a8
消息体标志	RTF 标志	HTML 标志	MIME 标志	0x3134 或者 0x313037(聊天室)
消息体格式	RTF 格式	HTML 格式	MIME 格式 UTF-8 编码	非通用格式, 采用 UTF-8 编码

例如 MSN 客户端给消息服务器发送一个即时文本消息的应用层协议格式为: MSG TrID N Length \r \nMessage

该消息中 MSG 是一个发送消息命令,命令之后是用空格隔开三个参数; TrID 是客户端与服务器交互的标志, N 是服务器响应的特征码,表示只要求服务器不能转发消息给接收客户端时才响应; Length 是消息长度; \r \n 是回车换行符,表示命令结束; Message 是指定长度的消息体。MSN 的 Message 消息体消息是一个 MIME 格式编码流,使用标准的 MIME 头,可以参考 RFC-1521 和 RFC-822 来了解更多的关于 MIME 格式的信息。

(3) 雅虎通的协议格式如图 6 所示。

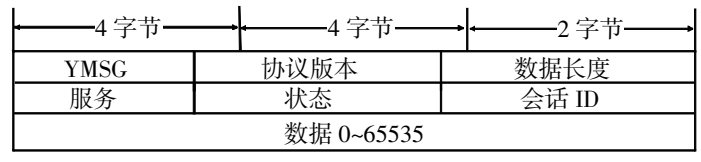

图 6　雅虎通协议格式

YMSG 为应用层首标,由 ASCII 表示; 其后的四个字节为客户端的协议版本号; 数据长度指出数据部分的字节长度; 服务是两字节的操作码,指明客户端发送的是哪一种服务请求或者说明服务器对哪一个服务的响应。雅虎通至少提供了 45 种以上的服务,发送一般消息的服务是 0x0006,聊天室消息的服务是 0x00a8; 状态在服务器响应的情况下,表示对请求的响应状态(成功,失败等) 。会话 ID 是客户端与服务器端通信的标志,一旦服务器指定它们之间的一个会话 ID 以后,它们之间的所有数据包都使用这个 ID 进行通信。

雅虎通的数据部分的长度由数据长度字段决定。数据体没有采用通用的数据格式,而是由一系列的关键字和数值对组成,一种关键字对应一个数据值。关键字和数据值的长度不定,一般用两字节序列 0xc080 作为分隔符,分开关键字和数据值。实际数据包中关键字的含义依赖于使用的服务。例如发送实时消息数据包中, 0x3134 对应的数据值是用户的文本消息,它与文本消息之间用 0xc080 字节隔开。如果数据包是发送给聊天室的消息包,则关键字 0x313037 对应的数据值是用户的文本消息。需要说明的是,用户的文本消息 (下转第 250 页)

Samba 服务器也允许使用未经加密的用户密码,但既麻烦又不安全[1]。

3.3 资源访问控制管理

经过身份认证表明该用户是一个合法的 Samba 用户,但对于 Samba 服务器上共享资源是否能够访问及访问的方式,Samba 服务器可以通过资源控制进行管理。资源控制管理主要考虑三个层面:①UNIX/Linux 系统中的哪些资源可以共享。②共享的资源对哪些主机或用户开放。③用户对共享资源的使用设置何种访问权限。对三个层面的管理主要通过设置 smb.conf 中的对应参数,如表 1 所示。限于篇幅,对于参数的具体含义可参见文献[5~7]。

表 1 资源控制管理三个层面的相关参数

层面一的参数	层面二的参数		层面三的参数
[客户机上显示的目录名]	admin users	allow trusted domains	writeable
path	host allow	host deny	browseable
comment	public	guest ok	read only
available	only guest	valid user	printable
	invalid user	write list	

3.4 日志管理

日志分为系统日志和 Samba 日志。日志中记录了大量有利于管理的信息。系统日志的设置与管理可参阅 UNIX/Linux 有关文献。这里主要讨论 Samba 的日志管理。Samab 服务器的日志用于记录 Samba 的使用情况,设置恰当的日志参数可以对 Samba 服务器进行事后监督,并进一步提高管理水平。在 smb.conf 的[global]节中可以设置有关日志参数[7]。

3.5 系统备份与恢复

当 Samba 服务器出现问题后,用户希望尽快恢复系统,使之正常工作。做到这一点,应当在 Samba 服务器正常工作时,对系统进行备份,以防患于未然。系统备份的方式可以通过本地完成,也可以远程操作。备份内容的选择上既可以是整个系统,也可以是仅与 Samba 服务器有关的配置文件和日志文件。完成备份工作后,一旦 Samba 服务器出现问题,就可以及时恢复。Samba 客户机的备份相对较简单,因为 Samba 对客户机只要求支持 TCP/IP,有必要的情况下,可对 Windows 用户进行备份。最后,着重介绍一下系统管理与维护工具的选取。以往在局域网内对 Samba 服务器的管理进行远程“遥控”时,需要在本机上手动对系统中的通信协议进行参数设置,这种方法不仅需要大量的时间进行安装和调试,而且维护工作也非常烦琐。并且常用的 Telnet 等命令是一种基于字符的应用程序,对于远程系统操作时很不方便。比较优秀的系统及 Samba 服务器管理工具有 Linuxconf 和 Webmin,推荐使用 Webmin 来管理 Samba 服务器。Webmin 是一个基于 Web 的 Linux 系统管理工具,功能强大,操作界面非常友好,安全性较高[7],是一个理想的对 Samba 服务器和 UNIX/Linux 系统进行远程管理的有力工具。在 Samba 服务器上安装 Webmin 后,既可以在本地实施操作,也可以远程操作,方法如下:

(1) 选取与 Samba 服务器联网的任何一台远程机器(Windows 系统或 UNIX/Linux 系统)。

(2) 在 Web 浏览器(IE 或 Mozila 等)地址栏中输入 Samba 服务器的主机地址及端口号,如 http://210.41.196.1:10000(Webmin 的默认端口),此时出现 Webmin 系统管理员 Admin 的认证窗口。

(3) 输入正确的用户名及密码,认证通过后,就可以使用 Webmin 图形化远程网络管理界面对 Samba 服务器进行管理与维护。

4 结束语

处于异构网络中的 Samba 服务器,方便了 Windows 和 UNIX/Linux 系统之间的资源共享,但是无法保证它的绝对安全,尽管它需要安全。因此,有效地对 Samba 服务器进行管理,将能够在很大程度上减少不安全的因素。为了使 Samba 服务器更加安全,有必要构建系统完整的 Samba 服务器管理体系,并从各个层次实施安全管理策略。在具体应用过程中,用户可以根据不同的安全要求,定制不同的安全管理方案。使用 Samba 服务器不仅应用方便,而且安全可靠。

参考文献:

[1] 邹念,唐宁九,林锋.用 Samba 实现 Linux 和 Windows 之间的文件共享[J]. 计算机应用研究,2002,19(1):152-153.

[2] 韩德志,鄢让.利用 Samba 实现 Linux 与 Windows 98 的资源共享[J]. 计算机应用研究,2001,18(5):131-134.

[3] 陈旭,温阳东. Linux 系统网络安全问题分析及对策[J]. 合肥工业大学学报 2002,25(3):396-397.

[4] Dominic Baines. Samba 技术内幕[M]. 沈立,等. 北京:机械工业出版社,2000.

[5] 谭良,等. Samba 服务器共享资源安全层次模型研究[J]. 计算机应用,2004,24(2):115-117.

[6] 肖文鹏. 高效架设 RedHat Linux 服务器[M]. 天津:天津电子出版社,2003.

[7] 宋利军. RedHat Linux 9.0 实用教程[M]. 北京:科学出版社,2003.

作者简介:

王杨(1971-),男,安徽芜湖人,讲师,在读硕士生,主要从事计算机网络技术研究;王朝斌(1970-),男,重庆忠县人,讲师,在读硕士生,主要从事计算机网络技术研究;钟乐海(1963-),男,四川广安人,教授,硕士生导师,博士,主要从事计算机网络教学和研究。

(上接第 245 页) 采用 UTF-8 的编码方式,因此支持中文,一般一个中文字符由三个字节表示。

4 小结

本文针对目前对即时通通信监控的需要,对 ICQ, AIM, MSN 和雅虎通等几个主流即时通软件最新版本的文本消息传输协议进行了分析、比较和说明,为进一步对这些软件的文本消息监控提供了依据,同时为这些软件协议的进一步深入分析,如文件传输、音频消息传送、视频数据传送、文件共享等协议的分析提供了参考。

参考文献:

[1] SCAR (ICQ v7/v8/v9) Protocol Documentation[EB/OL]. http://iserverd1.khstu.ru/oscar/families.html, 2003-06-13.

[2] Yahoo Messenger Protocol(v10)[EB/OL]. http://www.venkydude.com/articles/yahoo.htm, 2003-09-01.

[3] MSN Messenger Service 1.0 Protocol[EB/OL]. http://www.hypothetic.org/docs/msn/sitev1/index.php, 2003-09-02.

作者简介:

李远杰(1972-),男,讲师,硕士研究生,主要研究方向为网络安全、软件理论与应用;刘渭锋(1978-),男,硕士研究生,主要研究方向为软件理论与应用、网络安全;张玉清,副研究员,主要研究方向为网络安全;梁力,副教授,硕士生导师,主要研究方向为软件理论与应用。