即时通信研究综述

朱和平

(南京邮电大学计算机学院，南京 210003)

摘 要：对即时通信系统的网络服务模型、通信方式、防火墙和网络地址转换穿越及标准协议进行了深入分析，讨论了即时通信几种主要安全问题，并对即时通信的发展作了展望。

关键词：即时通信；IMPP；SIMPLE；XMPP；安全

引 言

即时通信是一种基于互联网应用的实时交互方式。网络上的用户可以利用IM软件实现文字、音频和视频等信息的即时传送，以及点对点的数据交换。1996年11月，四位以色列籍年轻人开发出世界上第一个即时通信软件ICQ，随后便出现各种各样的IM软件，如雅虎公司(Yahoo!)与微软公司分别推出Yahoo! Messenger和MSN Messenger。在我国，众多的中文版IM软件也被开发出来，其中1999年2月腾讯公司推出的OICQ获得成功(OICQ在2000年4月正式改为QQ)。2006年5月，QQ注册用户超过5.315亿[1]，是目前国内拥有用户最多的IM软件。较为流行的IM软件还有新浪UC、网易泡泡等。IM涉及到多种技术研究领域(TCP/UDP/IP/Sockets、P2P、C/S、Web、Web Service、多媒体音视频编解码/传送等)，是通信技术与计算机技术融合的结果。即时通信的出现是基于互联网通信方式的一次重大变革，因此对即时通信的研究有着重要的应用价值。

1 即时通信机制

(1)即时通信的定义和功能

一般地，即时通信定义为应用在计算机网络平台上的、能够实现即时的文本、音频和视频等功能的一种通信系统。广义的即时通信包括网络聊天室、网络会议系统等所有联机IM软件和应用；而狭义的即时通信一般指由一组IM服务器控制下的若干IM客户端软件组成的系统[2]。目前，主流IM一般面向个人用户，可以归类为CIM(Customer IM)；也有一部分IM(比如腾讯RTX)面向企业，可以归类为EIM(Enterprise IM)。EIM服务器由企业自主控制，与CIM相比较，EIM在管理和安全上要求较高。

IM系统有三项基本功能：

①通过IM软件为用户创建一个虚拟的身份；

②为用户建立了一个网络间点对点的连接；

③建立一个平台，并通过这个平台的多个接口提供各种服务。

(2)即时通信网络服务模型和特点

IM软件一般采用C/S(客户端/服务器)模式，IM服务器具有中心服务器功能，用来管理网络上客户端、中转客户端信息及帮助客户端建立直接连接等。IM客户端一般要先登陆服务器才能接受各种服务。通信时，由客户端发起连接请求，服务器担任中转者的角色，将网络包从发送方转交给接收方。由于客户之间使用音频、视频及传输文件等服务，通信数据量较大，此时由服务器转发会出现响应不及时、服务器负载过重等问题，因此，当提供这些服务时，通常由服务器进行协商，在两个客户端建立P2P(点对点)连接，进行直接传送。其通信服务模型如图1所示。这种模型构架简单，灵活，实际的IM软件一般都采用这种模型。

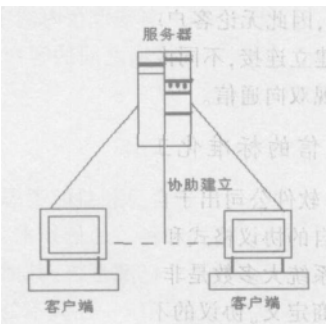

图1 IM软件的服务模型

(3)通信方式和通信传输协议

IM系统通信主要有两种方式，第一种是客户端之间通过服务器进行通信，第二种是客户端之间直接进行通信，即点对点通信。采用第一种方式时，服务器对网络进行监听，客户端在启动之后，主动去连接服务器的监听端口，由服务器派生新的工作线程处理和回应每个客户端的所有网络请求。这样，当两台客户端需要通信时，由服务器中转，将网络包从发送方转交给接收方。采用第二种方式时，客户端之间可以通过服务器协助或客户端直接建立连接进行点对点通信。IM通信传输协议有较多选择，目前一般使用TCP或者UDP通信协议。国内主流即时通信软件QQ、MSN等IM软件都是TCP和UDP的应用。TCP是面向连接的协议，在客户端和服务器进行通信之前，必须先建立连接，传输比较可靠、准确，但是效率不高，占用资源较多。UDP是无连接方式的协议，通信前无需建立连接，它的效率高、速度快，而且占用资源少，但是其传输机制为不可靠传送，必须依靠辅助的算法来完成传输控制。

(4)防火墙和网络地址转换的穿越

实现即时通信必须对网络上的一些特殊限制采取一些措施，以突破这些限制，其中最重要的一个方面就是穿越防火墙和网络地址转换(Network Address Translation, NAT)。互联网为了网络安全，采取了防火墙等网络安全技术，同时又因为网络地址资源日益紧张，促使了网络地址(端口)转换(NAT/NAPT)设备的大量使用，形成了许多使用私有地址的局域网段，划分了内网(防火墙或NAT设备保护的网段)和外网，并限制了网络访问方式，只有合法的网络端口/地址能够进出防火墙或NAT设备，同时也限制了外网段的节点主动发起的网络连接，使得外网的主动连接通信被阻挡。IM客户端要进行通信必须能够穿越防火墙和NAT。IM服务器一般架设在公网上，拥有固定合法的IP地址，因此无论客户端是否在内网中，都是可以与服务器建立连接，不同内网之间的客户端可以通过服务器实现双向通信。

2 即时通信的标准化工作

由于IM软件公司出于自身利益的考虑，均制定并保守着各自的协议格式和相关通信技术，所以目前的即时通信系统大多数是非标准系统，其通信协议与接口均由厂商定义。协议的不统一性和不公开性束缚着IM的快速发展，并造成各类IM软件不能互联互通及客户通信存在安全等问题。因此IM的标准和协议的统一是未来IM发展的必然趋势。IETF(Internet Engineering Task Force，互联网工程任务组)把IM划分为四种协议，即IMPP(即时信息和出席协议)、PRIM(出席和即时信息协议)、SIMPLE(针对即时信息和出席扩展的会话发起协议)及XMPP(可扩展的消息出席协议)。PRIM与XMPP、SIMPLE类似，已经不再使用。比较有影响的是SIMPLE和XMPP，二者都符合RFC2778[3]和RFC2779[4]。

(1)IMPP

为推动即时通信协议的标准化进程，IETF成立了IMPP工作组，并于2000年2月发布了描述IMPP基本框架与需求的RFC2778和RFC2779。RFC2778定义了所有出席信息和即时消息服务的原理，描述了IM的功能，正式为IM系统勾勒出了模型框架。RFC2779定义了IMPP的最小需求条件，并就出席信息服务(Presence Service)定义了一些条款，如运行的命令、信息的格式等。在RFC2778中，出席信息和即时消息系统被定义为允许用户相互订阅并通知状态改变，且用于用户间传送即时短消息。FC2778描述的出席信息和即时消息系统的抽象模型(Abstract Model)定义了两种独立的服务，即出席信息服务和即时消息服务(Instant Message Service)。出席信息服务负责出席信息的收集和分发，其服务模型中有两类客户：一类提供出席信息，称为出席者(Presentity)；另一类使用出席信息，称为观察者(Watcher)。其模型如图2所示。RFC2778没有要求专用的出席信息服务器，出席者和观察者之间可以直接通信，也可以采用代理转发。即时消息服务则负责接收和投递即时消息，其服务模型中也有两类客户：一类是寄送即时消息(Instant Message)，称为发送者(Sender)；另一类是接受即时消息，称为消息箱(Instant Inbox)。其模型如图3所示。RFC2778也没有要求专用的即时消息服务服务器，实际的即时通信系统中投递方式有较多种，可直接投递，也可经服务器中转投递。

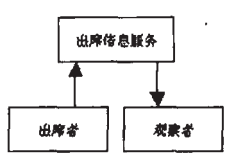

图4 出席信息服务模型

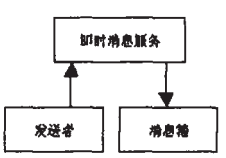

图5 即时消息服务模型

(2)SIMPLE

SIMPLE旨在将SIP协议应用于IM和出席检测

业务。SIP最初是一种视频会议的标准。SIP协议是由IETF提出的一种用于IP网络多媒体通信的应用层控制协议,其主要功能是创建、修改、终结和管理多媒体会话或呼叫。SIP协议的语法和语义在很大程度上借鉴了SMTP和HTTP的机制,使用C/S通信模式以及文本形式的消息编码。其优势在于编码效率高,特别方便音频、视频等多媒体应用,但在应用于IM时,SIP存在很多IM中并不需要的冗余功能及差错重传功能较弱等问题。SIP能够传送多种方式的信号,如INVITE信号和BYE信号分别用于启动和结束会话。SIMPLE是SIP即时消息和出席的扩展,其增加了NOTIFY、SUBSCRIBE和MESSAGE方法支持IM和出席业务。MESSAGE(消息)用来发送一次性的短消息,即寻呼机模式的IM。SUBSCRIBE(提交)用于申请者向服务器申请获得用户的出席信息,而NOTIFY(通告)用于向申请者描述该用户的出席信息[5]。较长IM对话的参与者需要传输多种延时信息,它们使用INVITE和消息会话中继协议(Message Session Relay Protocol, MSRP)。MSRP协议与SIMPLE协议结合,可用于IM的文本传输,正如RTP协议与SIP协议相结合,可以用于传输IP电话中的语音数据包一样。

(3)XMPP

XMPP是一种基于XML (Extensible Markup Language,可扩展标记语言)的传递出席信息和消息路由协议,它为不同网络之间互联提供了一种安全而简单的编程语言,是Jabber系统(一种开放源代码的IM系统)的基础[6]。一个XMPP实体可以是任何网络端点(如网络中的一个ID)、并能够用XMPP通信的事物,这一类的实体可以唯一编址。XMPP实体的地址被叫做Jabber标识符或JID。JID唯一确定进行即时消息和在线状态信息通信的独立对象或实体,并可兼容其他即时通信系统(如MSN等)相应的实体标识及其在线状态信息。一个有效的JID包括三个部分:域标识符,节点标识符和资源标识符[7]。域名指定了实体连接的XMPP服务器,每个可用的XMPP服务器都拥有一个完整域名,域名可在域名系统(DNS)中查找。节点可表示某用户、一类应用或某项服务,所有节点都对应一个精确的域名。资源用于识别属于用户的特殊对象(如设备),允许一个用户同时以多个资源与同一XMPP服务器连接。XMPP具有语法清晰、易于实现等特点,因其专门面向即时通信,具有即时通信特需的一些功能特性,如好友列表、群组功能等。XMPP协议已被批准为互联网即时通信协议标准。

3 即时通信的安全

IM同其他网络软件一样,也存在很多安全缺陷,如信息泄露、易受垃圾信息攻击等。目前,对IM信息安全研究已经取得一定的成绩,但很多方面还需要进一步深入研究。IM主要安全问题涉及以下几方面:

(1)穿透安全防御

大多数IM软件都可以突破类似防火墙这样常见的安全防御构件,允许用户选择使用的端口,甚至会自动尝试连接未被封住的端口,因此任何局域网内具有Web浏览权限的用户,都可以通过一个外部的代理服务器和特定的未被防火墙禁止的端口(如80, 23)等等,将信息发送到外部网络。在这种情况下,通过端口号限制非授权访问是不可能的,从而使得黑客可以利用即时通信工具绕过防火墙机制的保护,对防火墙所保护的网络和计算机造成破坏。

(2)病毒、木马等恶意软件

IM软件一般都提供文件传输的功能,通过点对点方式传送文件。因此受感染的文件就可以借此绕过防病毒网关的扫描,致使病毒、蠕虫和木马等恶意软件进入网络中的计算机。

目前通过感染IM系统实现传播的病毒主要呈现出以下几类形态:

①以占用系统资源、破坏目标系统及种植木马为目的(比如MSN"性感鸡"病毒);

②窃取IM系统账号密码及相关信息(比如QQ密码结巴);

③利用感染的IM系统发送各种消息的病毒(比如QQ尾巴)。

针对即时通信的恶意软件正在超越电子邮件病毒,成为应用系统的新的主要安全威胁。

(3)系统自身安全缺陷

IM基本上属于C/S或者P2P的应用。在P2P方式下,IM之间直接通信时,其IP地址很容易直接泄露给中间人和通信对方,成为遭受扫描和攻击的第一道缺口。P2P方式不经由IM服务器,易受到信息拦截攻击,使其不能进行正常通信。在C/S方式下,主要问题是服务器及其管理者不一定可信,可能成为中间人攻击的发起点。IM服务器中存储了大量的个人信息以及用户之间关系的信息,这些都属于个人隐私,如果IM服务器发生信息泄露就会造成大范围的伤害。

(4)帐号欺诈

IM软件一般需要用户输入帐号和密码,验证成功后方可使用服务。但几乎所有IM服务都采用了匿

名注册方式，这使得IM系统中的用户标识与真实的操作者无法对应，所以利用即时通信平台开展的非法入侵难于追查。一些不法者便利用这种机会实施网络诈骗。

其常见的诈骗行为主要有以下几种方式：

①实施攻击行为或恶意软件传播；

②利用窃取的账户信息向用户发送广告等不良信息；

③通过注册名字或含义令人误导的IM账号来冒充别人，骗取通信对方的信任，套取有价值的信息；

④通过各种手段窃取合法用户的账号等。

4 即时通信发展展望

IM最初只有发送即时文本信息等简单功能，此后陆续又具有文件传输、音视频聊天及网络游戏等更高级的功能。历经十多年，IM正在向新一代的综合即时通信演进，即从文本向语音、视频和多媒体，从固定网络向无线移动，从个人通信向企业即时通信和协作演进。随着计算机和通信技术快速发展，IM将提供的服务会更加丰富，网络虚拟社区将会普及，即时通信将更加凸显个人信息处理的能力，同时与社会文化和本地化应用将进一步深入融合。随着即时通信标准及安全的完善和发展，即时通信有可能实现各个通信系统之间的统一接入。目前，雅虎通(Yahoo! Messenger) 8.0版本已经实现了与Windows Live(MSN)互连互通。另外，即时通信将会进一步整合有线和无线业务，继续扩大增值服务功能的范围，如果政策允许，即时通信软件甚至有可能与固话互通。在安全方面，随着技术手段的不断突破，即时通信产品的安全性会进一步提高，稳定性日趋成熟。

参考文献

[1]http://www.tencent.com/about/about.shtml

[2]代印唐，张世永. 即时通信安全研究. 电信科学，2006，4

[3]M Day, J Rosenberg, H Sugano. RFC2778. http://www.faqs.org/rfcs/rfc2778.html

[4]M Day, S Aggarwal, Gmohr, J.Vincent. RFC2779. http://www.faqs.org/rfcs/rfc2779.html

[5]Jongbok Byun. Instant Messaging and Presence Technologies for College Campuses. IEEE Network, May/June 2005

[6]张云川. 标准化的即时通信协议. 武汉科技大学学报(自然科学版)，第28卷，第4期

[7]RFC3920. http://www.faqs.org/rfcs/rfc3920.html

(收稿日期：2006-09-11)

A Survey of Instant Messaging

ZHU He-ping

(Department of Computer and Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003 China)

Abstract: In this paper, firstly, the network service model and the communication method for IM systems are analyzed, and the traversal of firewall and network address translation (NAT) within IM systems and the standardized protocols for IM systems are studied. Secondly, some security problems of IM systems are discussed. Finally, several suggestions for the future development of IM systems are given.

Key words: Instant Messaging; IMPP; SIMPLE; XMPP; Security