国内即时通讯软件的安全脆弱性分析

A Discussion of Vulnerabilities of Security of Instant Messaging Softwares in China

彭　元[1]，黄皑昌[2]，庄军莲[1]

Peng Yuan[1]，Huang Aichang[2]，Zhuang Junlian[1]

（1. 广西科学院，广西南宁　530022；2. 广西工联工业工程咨询设计有限公司，广西南宁　530003）

（1. Guangxi Academy of Sciences，Nanning，Guangxi，530022，China；2. Guangxi Union-Industrial Engineering Consulting & Design LTD.，Nanning，Guangxi，530003，China）

摘要：即时通讯软件在网络协议上存在一定的安全隐患，IM 软件开发中涉及的多线程技术、服务器程序开发、数据库开发、脚本语言、组件开发技术等也会造成一定的安全隐患。IM 软件在使用过程中存在用户账号和密码易暴露，活链接功能、开放的端口及消息收发权限可能会被恶意利用等安全性问题。建议 IM 软件开发商建立软件用户数据加密保护体系，提醒用户注意密码等用户私有信息的安全性；开发相应的软件插件，接受用户对恶意链接投诉，并由系统自动将其屏蔽；加强与杀毒软件开发商的合作，及时提供升级病毒库；在服务器运行先进的网络入侵监测系统，防范开放的端口及消息收发权限被恶意利用。

关键词：即时通讯软件　安全　脆弱性

中图法分类号：TP393.08　　**文献标识码**：A　　**文章编号**：1002-7378(2005)03-0189-04

Abstract：The recentstudies indicate that there are some potential security bugs in the network protocol of Instant Messaging (IM) softwares. The situation would be worse when disadvantages of multithreading, the server process, database system, script language and module in IM development are considered. For instance, usernames and passwords in IM softwares can be showed up easily, and active link, open port and the authorization of received and sent news may be used balefully. Software developers should (1) establish safety and security systems to protect users' databases, (2) alarm users to pay attention to their private information such as passwords, (3) provide correlative module and investigate the complaint of baleful linkage which should be shielded immediately by the system, (4) of internet service, the advanced monitor system for internet invasion should be run in server to prevent baleful usage of open port and the authorization of received and sent news.

Key words：instant messaging software，security，vulnerability

即时通讯(Instant Messaging，简称 IM)能使两个在线的人相互同意联系后，通过文本、语音、图片、视频等方式进行交流，可直接传送文字、电子文档、声音、影像给对方，具有比电子邮件更快捷，更具交互性，比手机、电话更有可记录性、费用低、数据形式多样化、传送数据量无限制性等优点。目前 IM 技术已被广泛应用到与信息传递相关的各行各业，成为现代信息交流的一种优选手段。但是，随着 IM 的广泛运用，IM 也成为了病毒和蠕虫、身份盗用和身份欺骗、数据安全性暴露、防火墙隧道、以及垃圾信息的潜在源头，IM 带来的网络安全问题变得异常严峻，其安全态势不容乐观。2005 年第一季度 IM 安全威胁比 2004 年第一季度增加了 271%；2005 年 3 月份共发现 48 个安全威胁，比 1 月份和 2 月份的总和(30 个)还高 50%以上，其中多数攻击是针对 IM 客户软件的蠕虫，且蠕虫形式越来越复杂[1]。

收稿日期：2005-05-29

作者简介：彭　元(1970-)，男，广西临桂人，助理工程师，主要从事计算机网络安全研究工作。

随着国内办公局域网、小区宽带等计算机网络环境的不断发展，IM 已在人们的工作和生活中起到越来越重要的作用。2004 年中国有即时通讯用户 6272 万人，2005 年将达到 8267 万人，2006 年将达到 10334 万人，国内用户最常用的即时通讯软件是腾讯 QQ，其次是 MSN、网易泡泡和雅虎通[2]。因此，分析国内 IM 软件存在的安全问题，研究 IM 的安全脆弱性，能促使软件开发商和使用者采用有效的手段，避开可能带来的网络安全事件，使 IM 技术得到更为成熟的应用和发展。

1 IM 软件出现安全隐患的原因分析

目前的 IM 软件大都优先支持用户数据报协议 UDP[3]（UDP 在 RFC768[4]中有具体描述）。UDP 和传输控制协议 TCP[3]（TCP 在 RFC793[5]中有具体描述）都属于传输层协议，但 UDP 是一种支持无连接的传输协议，即计算机进行数据传输的时候，发送方只需要知道对方的 IP 地址和端口号就可以发送数据，而并不需要进行连接，它并不提供数据传送的保证机制。这就在带来高速便捷连接的同时，也给基于 UDP 编写的程序带来了一个必然的缺点：即数据包传输不可靠，丢包率高。当然，在目前网络速度和通信质量已经有了很大提高的情况下，对于一些即使丢失若干数据包也不影响整体性的数据传输，如音频数据，视频数据等，采用 UDP 还是很好的选择。因此，如 OICQ 和 ICQ 等 IM 软件，往往都优先支持 UDP。他们看中的都是 UDP 具有对网络资源占用少，数据处理速度快的优点，但是开发时往往忽视了数据安全性不高的缺陷。例如，早期的 OICQ 软件，分为 Client 和 Server 两个部分，Client 部分由用户运行，Server 部分在腾讯公司主机上完成。Client 和 Server 之间通讯采用 UDP 协议，Client 采取本地端口 4000、远程端口 8000 的 UDP 封装。Server 返回信息采用本地端口 8000，远端端口 4000 的 UDP 封装。由于 UDP 协议不保证数据肯定发送到远端，客户端在收到服务器回应前，会反复广播 UDP 消息，如无响应再通过服务器广播，在得到目标用户的回应后最终得到对方 IP 地址。

IM 软件会暴露用户的 IP 是一个安全隐患，同时，由于产生一个任意源地址的 UDP 包很容易实现，采用 UDP 是可以制造伪消息并传递的，这也是一个较为严重的安全隐患。另外，初始的 IM 软件的所有数据通讯往往都在 UDP 下用明文传送，包括用户资料，信息内容，密码等等，均没有使用加密协议，使得 IM 用户安全受到极大威胁。

由此可见，IM 软件仅从网络协议上考虑就存在着一定的技术安全隐患，如果再加上 IM 软件的开发要涉及的多线程技术、服务器程序开发、数据库开发、脚本语言、组件开发技术等等，就会有更多的安全隐患。

2 IM 软件的安全脆弱性主要表现

2.1 用户账号和密码的安全隐患

IM 软件的用户帐号和密码能够通过本地 Windows 系统直接获得，手段之一是通过破解保存在本地硬盘上的密码信息文件获取密码。例如对于 QQ，盗号者可以用一些密码暴力破解软件轻易获取密码，如“QQ 密码暴力破解器”就支持在其默认“字典”中进行破解，还可以手动更新 password.ini 字典文件。此类方法不需要登录服务器，只要在本地将加密后的口令与 Shadow 文件中的口令相比较就能非常容易地破获用户密码，尤其对那些口令安全系数极低的用户，更是在短短的一两分钟内，甚至几十秒内就可以破解。手段之二是绕开密码直接查看用户信息。例如陆续出现的“登录密码修改专家”、“QQ 任我行”、“QQsuperKey”和“QQ 免密码登陆器”等黑客工具，都可以绕过本地密码验证系统，离线登录，查看其聊天记录、好友列表。利用这些工具，甚至不用密码，就可以毫无顾忌地探测查看用户留下的个人隐私。手段之三是利用软件对本地用户缺乏认证体系的漏洞，直接将非法用户信息转存入合法用户帐户中，获得合法的查看权限。例如，有本地用户 1 和 2，1 用户想察看 2 用户的好友名单，按个人隐私的安全要求，如果没有用户 2 的同意（即以用户 2 的密码进入），用户 1 是不应该得到任何资料的。实际上，用户 1 只要把用户 2 的帐户文件夹打开（默认为 C:\Program Files\Tecent\2 下），将其中的 User.db 文件复制到自己的合法账号下的文件夹（默认为 C:\Program Files\Tecent\1）中，再用自己的合法密码登录该帐号，这时用户 2 的好友列表会自动加入用户 1 的好友栏内，毫无隐私可言了。可见某些 IM 软件的数据文件对本地用户身份是不加验证的，这就给获得本地用户的个人信息敞开了一扇大门，这将导致个人隐私和商业机密被恶意泄露的可怕局面。

2.2 IM 软件的活链接功能被恶意利用

用户收到好友发来的 IM 消息中常常会带有 IM 软件的活链接，例如一个网址，用户只要直接点

击该网址就能立即调用 IE 等浏览器，进入该网页。由于该功能操作便捷，被很多病毒利用，病毒运行时会利用聊天窗口向所有在线好友发送一个病毒网址的活链接，当好友误以为是有用网址而点击时就会中毒，从而使病毒得到广泛传播。

这种病毒是利用用户对 IM 软件的熟悉和信任，在某个网页上嵌入了一段恶意代码，通过系统的自动运行，达到侵入用户系统，进而进行病毒复制和发送的目的。这类病毒在 IM 软件里的存在数量大、变种多的特点，并且由于该类病毒文件除了利用 IM 进行再次传播外，同时还会利用 IM 软件本身漏洞，采用缓冲区溢出、拒绝服务等攻击方式，对整个网络系统进行攻击，因而产生了极为恶劣的影响。例如早期针对 MSN Chat control 中存在 unchecked buffer 漏洞[6]，攻击者编写了如下恶意代码：

```
<object classid="clsid:9088E688-063A-4806-A3DB-6522712FC061" width="455" height="523">
<param name="_cx" value="12039">
<param name="_cy" value="13838">
<param name="BackColor" value="50331647">
<param name="ForeColor" value="43594547">
<param name="RedirectURL" value="">
<param name="ResDLL" value="AAAAAA[27,257 bytes is where the EIP starts]">
</object>
```

攻击者将上述代码文件保存为 html 文件，再将这个页面文件上传到空间里得到 URL 地址，然后将这个 URL 地址作为活链接发送给欲攻击的 MSN 用户，对方一旦点击这个活链接，就会发生缓冲区溢出，导致 MSN 非法关闭。

与以往不同的是，目前的蠕虫发展趋势越来越智能化，一种新的趋势是：蠕虫运行感染机器后，会立即在该机上自动架设一个简易 http 服务器，然后启动新线程，在新线程中寻找 IM 软件的发送窗口，一旦找到，它就会通过设置消息文本框的内容并控制发送按钮来达到发送恶意信息的目的。目前，这类恶意信息已经发展成为木马入侵的常用工具。例如“QQ 叛徒”（也叫“远控精灵”）就是一个通过监视 QQ 的消息来进行远程控制的木马。其原理是：病毒通过活链接等方式被植入对方计算机后，将随时检测该机 QQ 接收到的消息，当出现预设的特殊字符时，则进行对应的操作，实现远程控制。该病毒具有很大的隐蔽性，它不新开通讯端口而使用合法端口，这样的控制方式可以使大多数防火墙失效，极具欺骗性。该病毒可以执行的操作包括：上传、下载、执行文件，共享硬盘，关闭、重启计算机，抓屏并发送 E-Mail，通过进程名或 ID 来终止进程的运行，关闭、卸载木马等，造成的影响极其恶劣。

2.3 开放的端口及消息收发权限被恶意利用

大多数 IM 软件都是通过公开的端口进行信息传送的。如：MSN 通过 1863 端口进行信息传输，QQ 通过 4000 端口，而 Yahoo 用的是 5050 端口。这些端口属于 UDP 端口，在可以实现直接传送消息的同时，也存在着各种漏洞，IM 软件很容易因为这些开放的端口而受到病毒或黑客攻击。比如 Worm_Witty.A 蠕虫病毒就是利用 4000 端口直接向随机 IP 发送病毒，并且伪装成 ICQ 数据包，造成的后果就是向硬盘中写入随机数据。还有像 Trojan.SkyDance 特洛伊木马病毒以及“QQ 蜗牛炸弹”等类的病毒也都是直接对端口进行攻击或者利用 4000 端口进行欺骗攻击的。

在 IM 软件中，信息的发送及接收都应该有相应的权限设置，如果这些权限设置处理不当，必然会存在很多不安全的因素。比如曾经出现的“QQ 炸弹”，就是恶意用户利用对特殊字符发送的漏洞，使用大字体导致 Riched20.dll 文件缓冲区溢出[7]，其主要攻击代码如下：

```
{\rtf1\ansi\ansicpg936\deff0\deflang1033\deflangfe2052
{\fonttbl
{\f0\fnil\fprq2\fcharset134\'cb\'ce\'cc\'e5;}
}
{\colortbl;\red255\green0\blue255;}
\viewkind4\uc1\pard\cf1\kerning2\f0\fs180000000000000000000000000000000000
www.abcd.com\abc
}
```

在这段攻击代码中，“\fs”是用来设置后面文字的字体大小的，当字体大小数字串长度超过 32 字节时，就会引发缓冲区溢出，当超过 34 字节以后就有可能导致应用程序崩溃，很多 IM 软件都受过此漏洞影响。

消息收发权限被恶意利用后，“万箭攒心”等类型的攻击软件可以轻易实现不通过对方验证而直接

给对方发送垃圾邮件或者给对方自动重复发送大量信息，造成消息攻击，迫使对方下线或系统崩溃。

3 IM软件的安全对策及建议

防范IM软件的安全隐患，首先，软件开发厂商必须建立起本地用户数据的加密保护体系，尽可能地提醒用户注意密码等用户私有信息的安全性；用户也要有密码和数据保护的安全意识，要考虑密码设置是否为强密码，密码要定期更换，不要轻易在聊天室、论坛等公开场合留下用户ID。在公共场所使用共用计算机时，尽可能不要在本地保存用户数据，在离开计算机时，应该删除相应的用户文件夹。目前一些IM软件已意识到本地用户数据的安全性问题，已经设置了在用户下机时提醒用户删除本地用户所有信息的功能。其次，对于IM软件的活链接功能被恶意利用等类问题，建议软件开发商建立一套恶意链接举报机制并开发相应的软件插件，当用户发现一些不良链接时，可以直接向软件服务商投诉，由IM软件的服务商利用相应软件进行测试后由系统自动将问题链接在服务器上进行屏蔽。同时，IM软件厂商还应该加强与杀毒软件开发商的合作，将发现的恶意代码的病毒特征功能及时通报给所有杀毒软件开发商，由杀毒软件厂商及时提供升级病毒库，提供给广大用户及时升级杀毒软件。当然，作为用户来说，对所使用的软件操作系统和IM软件，要尽可能使用最新版本，并且也不能完全依赖操作系统和IM软件自身的安全措施来防毒防盗，要安装防火墙和杀毒软件，启动恶意代码等的实时监控系统，经常更新病毒软件，这样才能较好地防范各种针对IM的恶意攻击。在使用IM软件时，不要轻易打开任何链接，特别是一些无法判断身份的消息，就算是好友发来的链接，也必须再次询问，在得到好友再次确认后方可点击，以免遭受病毒的感染。另外，用户要注意有条件地使用IM软件提供的在线传输功能，对无法确认来源和信任度的文件传输，要拒绝接收。对于已经接受的可信任文件，在打开(运行)前，最好经过杀毒软件的扫描检查。最后，对开放的端口及消息收发权限被恶意利用的隐患，IM软件开发商应该在服务器运行先进的网络入侵监测系统，对某一时段突发的针对开放端口的IP地址扫描以及大数据流进行监测，一旦发现高频率地同一消息的反复发送，必须在服务器端终止该线程，达到防范恶意攻击的目的。对于用户来说，最好使用代理服务器模式并使用隐身登录，同时尽可能将用户信任模式设为需要通过身份认证的形式，这样，攻击者无法得到真实IP，也就无法对端口进行直接攻击了。这对"QQ蜗牛炸弹"和"万箭穿心"等端口攻击软件是十分有效的。

当然，IM软件的安全性还有其他的方方面面，随着IM软件运用的不断深入，可能会有更深层次的问题暴露出来，但是只要软件厂商和用户都能够积极对待IM软件的安全脆弱性问题，提高安全防范技术和安全管理意识，基于IM的网络安全是会有保证的，IM作为一种新兴通讯手段将会得到更大发展。

参考文献：

[1] Gregg Keizer. IM and P2P Malware Threats Nearly Triple[EB/OL]. http://www.techweb.com/wire/security/160500554,2005-6-6.

[2] 艾瑞市场咨询. 2004年中国即时通讯简版研究报告[EB/OL]. http://www.iresearch.com.cn/instant_messenger/detail_free.asp?id=11617,2005-06-06.

[3] Andrew S Tanenbaum. 计算机网络[M]. 熊桂喜，王小虎，译. 北京：清华大学出版社，1999.

[4] J Postel. RFC 768[EB/OL]. ftp://ftp.rfc-editor.org/in-notes/rfc768.txt,1980-8-28.

[5] J Postel. RFC 793[EB/OL]. ftp://ftp.rfc-editor.org/in-notes/rfc793.txt,1981-9.

[6] Microsoft. Microsoft Security Bulletin MS02-022[EB/OL]. http://www.microsoft.com/technet/security/bulletin/MS02-022.asp,2003-2-28.

[7] 万 涛. 漏洞终极攻防战[M]. 济南：山东电子音像出版社，2004.

(责任编辑：邓大玉 韦廷宗)