学 号 2012201101

密 级

哈尔滨工程大学学士学位论文

安全聊天工具的设计与实现

院（系）名　称：软件工程学院

专　业　名　称：软件工程

学　生　姓　名：孙雪峰

指　导　教　师：史长亭 讲 师

哈尔滨工程大学

2017年6月

**安全聊天工具的设计与实现 孙雪峰 哈尔滨工程大学**

学 号 2013201213

密 级

安全聊天工具的设计与实现

Design and Implementation of Student's Dormitory Management System

学生姓名：孙雪峰

所在学院：软件工程学院

所在专业：软件工程

指导教师：史长亭

职称：讲 师

所在单位：哈尔滨工程大学

论文提交日期：2017年6月

论文答辩日期：2017年6月

学位授予单位：哈尔滨工程大学

摘要

在使用聊天软件的过程中，特别是在商业、科研、军事等对于保密性要求较高的领域，传递消息的安全性一直是用户比较关心的问题。为了提高用户使用即时通信工具时个人通信数据的安全性，降低用户通信信息被泄露的风险，本文设计并实现了安全聊天工具。

安全聊天工具通过SuperSocket服务器框架与MySQL数据库组合搭建服务端，使用自定义的起止符协议完成通信，设计并实现了SuperCLient框架来实现系统的客户端。在安全性保证策略方面，以RSA加密算法为核心，基于数据加密传输、身份验证增强、SQL防注入、阅后即焚这四种安全策略，并完成了身份验证、消息通信、用户信息管理、好友信息管理等功能。经过反复的测试系统安全性能良好，通过各种安全策略协作，有效的保护了用户聊天信息的安全，极大的降低了用户在聊天过程中信息泄露的风险。

关键词：即时通信；信息泄露；安全策略；RSA算法

**ABSTRACT**

During using the chat software, especially in the business, scientific research, military and other areas of high confidentiality requirements, the security of instant messaging has always been a concern for users. In order to improve the security of personal instant messaging and reduce the risk of leakage of users' communication information, this paper designs and implements a security chat tool.

Security chat tool through the Supersocket which is a server framework and MySQL database combination to build the service, using a custom protocol that fixed by head and tail letter to complete the communication. It designs and implements the framework of Superclient to implement the system client. In the Security assurance strategy, RSA encryption algorithm is the core, based on data encryption transmission, authentication enhancement, SQL injection, burn after reading these four kinds of security strategy, and completes the user authentication, message communication with friends, user information management, friend information management. After repeated testing system security performance is perfect, through a variety of security strategy collaboration, effectively protect the user chat information security, greatly reduced the user in the chat process information leakage risk.

**Key words:** Instant messaging; Information leakage; Security policy; RSA algorithm

目录

[第1章 绪论 5](#_Toc483172121)

[1.1 安全聊天工具研究的背景和意义 5](#_Toc483172122)

[1.2 国内外研究现状 5](#_Toc483172123)

[1.3 论文的主要研究内容 7](#_Toc483172124)

[1.4 论文的组织结构 7](#_Toc483172125)

[第2章 系统通信架构的设计 8](#_Toc483172126)

[2.1 基本架构与开发平台的选择 8](#_Toc483172127)

[2.2 服务器与数据库的数据交互设计 9](#_Toc483172128)

[2.2.1 数据库设计 9](#_Toc483172129)

[2.2.2 数据库操作接口的规定 10](#_Toc483172130)

[2.3 应用层通信协议设计 10](#_Toc483172131)

[2.3.1 起止符通信协议的设计 10](#_Toc483172132)

[2.3.2 服务端与客户端之间通信接口的规定 12](#_Toc483172133)

[2.4 服务端数据解析与分发设计 12](#_Toc483172134)

[2.5 客户端的SuperClient框架设计 13](#_Toc483172135)

[2.5.1 SuperClient框架概述 13](#_Toc483172136)

[2.5.2 SuperClient框架的使用方法 14](#_Toc483172137)

[2.5.3 SuperClient的数据通信原理 15](#_Toc483172138)

[2.6 多线程通信 16](#_Toc483172139)

[2.7 本章小结 16](#_Toc483172140)

[第3章 安全性保证策略 17](#_Toc483172141)

[3.1 数据加密传输策略 17](#_Toc483172142)

[3.1.1 加密算法的选择 17](#_Toc483172143)

[3.1.2 RSA加密算法的基本原理 17](#_Toc483172144)

[3.1.3 公钥与私钥在系统中的应用 19](#_Toc483172145)

[3.2 身份验证增强策略 20](#_Toc483172146)

[3.3 SQL注入防御策略 21](#_Toc483172147)

[3.3.1 SQL注入的基本原理 22](#_Toc483172148)

[3.3.2 关键词过滤 22](#_Toc483172149)

[3.3.3 参数绑定 22](#_Toc483172150)

[3.4 阅后即焚安全策略 23](#_Toc483172151)

[3.5 本章小结 24](#_Toc483172152)

[第4章 安全聊天工具的详细设计与实现 25](#_Toc483172153)

[4.1 系统功能模块的设计与实现 25](#_Toc483172154)

[4.1.1 初始化模块 25](#_Toc483172155)

[4.1.2 身份验证模块 25](#_Toc483172156)

[4.1.3 消息通信模块 26](#_Toc483172157)

[4.1.4 用户信息管理模块 28](#_Toc483172158)

[4.1.5 好友管理模块 29](#_Toc483172159)

[4.2 系统安全性能测试 30](#_Toc483172160)

[4.2.1 数据加密传输测试 31](#_Toc483172161)

[4.2.2 身份验证测试 31](#_Toc483172162)

[4.2.3 SQL注入防御测试 31](#_Toc483172163)

[4.2.4 阅后即焚功能测试 31](#_Toc483172164)

[4.3 本章小结 31](#_Toc483172165)

[结　　论 33](#_Toc483172166)

[参考文献 34](#_Toc483172167)

[攻读学士学位期间发表的论文和取得的科研成果 35](#_Toc483172168)

[致　　谢 36](#_Toc483172169)

# 第1章 绪论

1.1 安全聊天工具研究的背景和意义

2017年5月 12日，一种叫做WannaCry 勒索病毒利用NSA（National Security Agency，美国国家安全局）泄露的危险漏洞“EternalBlue”（永恒之蓝）进行传播[1]。截止2017年5月15日，WannaCry造成了至少有150个国家受到网络攻击，已经影响到金融，能源，医疗等行业，造成严重的危机管理问题。中国部分Windows操作系统用户遭受感染，校园网用户首当其冲，受害严重，大量实验室数据和毕业设计被锁定加密。这个最近广受关注的事件的发生也为人们敲醒了警钟，信息安全隐患这个看起来遥不可及的事情绝不是危言耸听，而是实实在在关系着每一个人的生活。

在当今这个信息爆炸的时代，教育、经济、军事、科技等领域都不可避免的要每天进行大量的数据信息交换。这些领域的信息交互就需要即时通讯工具来完成。然而在国内，用户较为熟悉的即时通讯工具也就是QQ、微信等工具，但是这些工具的安全问题又有较大的隐患，并不能保证学术研究、商业决策、军事机密、科学研究等等对于安全性要求极高的领域的需求。

所以，本文旨在设计开发一款安全性高、性能稳定的安全聊天工具。满足用户的即时通讯的基础上，通过功能和技术上的设计来保证用户聊天数据的安全性。有了这样一款安全聊天工具，就可以让各个领域的机密数据的即时通讯需求，并且尽可能的降低用户重要信息的泄露的风险，让消息更加安全的传递到用户手中。

1.2 国内外研究现状

对即时通信工具的安全性保证的研究从未走出过公众的视野，近几年国内外对于各种即时通讯工具的研究和关注也一直在进行当中。在2014年11月5日的一篇研究报道是近几年可信度较高且比较全面的评测[2]。纽约非盈利独立新闻机构Propublica高级记者茱莉亚·安格文(Julia Angwin)、普林斯顿大学安全专家约什·布内奥(Joseph Bonneau)以及电子前沿基金会技术专家彼得·埃克斯利(Peter Eckersley)联合对当前即时通讯工具的安全性进行了评测。结果发现，腾讯QQ安全性最差，得分为零。

研究人员列出了7条技术标准，以对通讯工具进行排名。这7条标准是：传输过程中是否加密、加密后服务商还能否读取、用户是否能够确认联系人身份、如果密钥被盗过往信息是否安全、代码是否开放供独立审查、安全设计是否合理存档、代码是否审查。

制定这些标准的目的是评估通信工具在设计时是否能够应对秘密内置在软件中的后门、互联网入侵等威胁。

评审的结果显示：得分最高的通讯工具之一是Cryptocat。Cryptocat是一项免费聊天应用，可以安装在网页浏览器中，它得到7分。这款应用因被《卫报》记者格兰·格林沃德(Glenn Greenwald)在香港与斯诺登会面时使用而名声大噪。旧金山公司Open Whisper Systems的三款手机应用也得到了最高的7分，他们是iPhone电话通讯安全应用Signal、Android电话通讯安全应用RedPhone、Android手机短信安全应用TextSecure。这三款都是免费应用，而且相对易于使用。苹果聊天应用iMessage得到了5分，Facebook chat、Skype、WhatsApp、Google Hangouts等流行应用大都在2分。腾讯QQ和南非即时通讯软件Mxit垫底，均得到零分。

而在我国的各种即时通信产品中，近几年在保证用户安全方面取得了明显的进步。比如在国内根深蒂固的QQ即时通讯软件，提供了登录手机验证、异地登录提醒、QQ安全中心以及详细的安全指导手册来保证用户个人信息的安全。还有近几年比较火热的聊天工具微信也深得人心，无论是移动端或者是PC端都强制用户通过手机扫码登录，如果环境检测异常还会要求用户通过手机验证码来验证用户身份。而微软MSN和阿里旺旺近年在保障用户安全方面取得了显著进步，技术和运营经验也有一定积累，未来仍有提升空间。对于MSN而言，应在优化客户端安全性能和提供更为便利的客服方面有所突破，并且建设本地化的安全宣传阵地;而阿里旺旺未来需进一步丰富用户安全教育手段，保持教育渠道通畅。TOM-Skype在安全服务等方面与行业领先者还存在差距。百度Hi作为即时通讯市场的新进入厂商，其安全体系处于构建初期，基础安全特性和服务体系有待完善。

尽管如此，用户的个人数据安全问题仍然没有得到彻底的解决，每年都有用户数据被泄露的新闻出现。2011年，中国最大的最大的IT社区和服务平台被攻击，其数据库中被其存储的600万个用户的明文密码公布到了网上。2014年，雅虎的个人用户的密保问题的答案，乃至一些个人专门开设的，毫无规律可循的二次加密密码被盗取。2017年5月份，一种叫做WannaCry 勒索病毒在全球肆虐，至少有150个国家受到网络攻击，成千上万的用户数据被病毒锁定，无法使用，已经影响到金融，能源，医疗等行业，造成严重的危机管理问题。由此可见，在各种系统中，数据通讯与存储的安全性问题一直存在且没有得到彻底的解决，而人们对于安全的需求却日渐迫切。所以，在此基础上，本文进行了基于安全保障的即时通信的研究，尝试探求一种安全的即时通信的方式来保证用户数据的安全。

1.3 论文的主要研究内容

本文研究的是保证用户信息安全的安全聊天工具的设计与实现。在安全聊天工具中，

聊天信息的交换功能是系统的基础，而保证用户聊天信息的安全是整个系统的核心。所以，本论文在完成系统基本的通信、管理等功能的基础上，还需要设计并实现若干种安全性保证策略来保证数据在传递过程中以及在客户端解析时的数据安全，完成了一款安全性高，性能稳定的安全聊天工具的设计与实现的相关工作。

1.4 论文的组织结构

本文共分为4章，按照系统设计的主次来划分，具体组织方式如下：

第1章主要讲述了安全聊天工具的研究背景和研究的意义、国内外对于安全即时通信的研究现状以及论文的主要研究内容的总体概述。

第2章从应用层通信协议的设计、数据库的表结构和接口设计、服务端的数据解析和分发以及客户端的数据解析和分发这4个角度来解释整个系统是的所有数据通信线路的设计与实现方式。

第3章着重阐明了本系统采用了哪些安全策略来保证用户聊天信息的安全性的。

第4章则以全局的视角来解释安全聊天工具的各个功能模块是如何实现。还展示了系统的功能测试和安全性能测试的结果。

最后是结论部分，对于整个安全聊天工具的设计与实现的过程予以总结。

# 第2章 系统通信架构的设计

显而易见的，通信功能是安全聊天工具最主要的功能。而对于系统的各个模块之间来说，如何实现数据交换也是最重要的部分。所以，本章主要讲述服务端与客户端、客户端的工作线程与UI线程、服务端与数据库之前的数据通信架构的设计工作。包含通信协议的制定、服务端与客户端的数据解析与分发、线程间通信技术、数据库操作等架构的设计。完成了这些模块的通信的方式和协议的制定，系统的开发的就有了大致的方向。

2.1 基本架构与开发平台的选择

首先来讲述系统的基础架构的选择，只有选择了合适的架构，才能在接下来的开发中一帆风顺。B/S架构与C/S架构是比较常见的两种系统架构方式。安全聊天工具的系统架构选择的是C/S架构并且使用winform开发平台，下文针对两种架构的特点以及系统的需求解释对于基础架构方式的选择的理由。

C/S架构也就是Client与Server模式，需要自己开发服务端和客户端，并且需要自己定义应用层通信协议，然后使用Socket网络通信接口来传递数据[3]。使用C/S架构的特点是在服务端和客户端端都可以完成较为复杂的业务逻辑，客户端自由度较高，可以胜任复杂的视图效果。这样对于服务端来说，运行数据负荷大大减轻，间接提升系统的性能。同时，C/S架构系统的开发的自由度较大，可以定制或者直接使用各种特点的应用层协议，满足各种用户需求。另外，基于Socket来实现服务端与客户端的长连接是十分的简单的，这一点对于即时通信类软件的开发是十分有好处的。同时C/S架构的自由开发与功能强大也是付出了很大的代价。比如开发的应用需要针对操作系统来开发，对于跨平台开发十分不友好。并且因为每一台用户机上都装有客户端，这对于系统的维护和更新的成本也相对较高。不过，对于安全聊天工具来说，windows平台足以应对大多数的应用场景，此外服务端与客户端的长连接以及用户数据的安全性也是强需求。由于本系统对于安全性能有较高的优先级，所以C/S架构的缺点也可以接受。

B/S可以理解为C/S架构的具体实现，即使用浏览器作为通用的客户端，基于HTTP应用层通信协议，在服务端也有tomcat、nginx等成熟的程序可以使用。所以，在完成一款基于B/S架构的web应用的设计的过程中，对于通信架构的设计成本就大大减少了。除此之外，B/S架构中只有极少的业务逻辑需要在前端实现，绝大部分的事务逻辑都在服务端来进行，这样就大大降低了客户端电脑的负载，也减轻和降低了系统维护和升级的成本和工作量。但是，这种设计成本的减少同样会引入一些不可回避的问题。第一、在B/S架构中，HTTP协议是基于短连接的，想要实现即时通信这类需要保持长连接的的开发成本较高；第二、使用B/S架构会暴露系统的服务器地址，导致系统的安全行出现隐患。由于B/S架构这两点问题的存在，在选择安全聊天工具的基础开发架构的过程中，C/S架构的安全性以及开发选择的自由性更胜一筹。

综上所述，使用C/S架构可以自定义应用层通讯协议，容易实现长连接，安全性更容易保证，C/S架构更适合安全聊天工具的开发。而在开发平台的选择上，C#拥有反射、委托等优秀的特性来支撑数据分发等功能需求，开发文档全面以及SuperSocket这样的优秀开源框架这些特点，更适合本系统的开发。

2.2 服务器与数据库的数据交互设计

2.2.1 数据库设计

安全聊天工具涉及的实体的数目较少，主要有用户、用户的好友这两个实体。本系统中的用户使用用户名、密码、私钥签名来验证身份，用户有昵称、头像、签名等个人信息。此外，用户要保存自己的好友用户名、好友备注等信息。为了聊天数据的进一步的安全，在本系统中不提供存储聊天记录的功能。综合以上的分析，安全聊天工具设计两张数据表。

1. 用户信息表（user）

用户信息表用来存储用户的个人信息，包括用户名、密码、公钥、昵称、个人签名

等信息。其中用户名作为主键，用户信息表如表2.1所示。

|  |  |  |  |
| --- | --- | --- | --- |
| 字段 | 字段类型 | 字段描述 | 备注 |
| U\_Username | Varcher(50) | 用户名 | 主键，非空 |
| U\_NickName | Varchar (20) | 名字 | 非空 |
| U\_Public\_Key | Varchar (255) | 公钥 | 非空 |
| U\_Password | Varchar (50) | 登录密码 | 非空 |
| U\_SignaTure | Varchar (100) | 个性签名 | null |
| U\_HeadPic | Varchar (50) | 头像地址 | null |

表2.1 用户信息表

1. 好友信息表（friends）

好友信息表用于存储用户的好友信息，包括用户名、好友用户名、好友备注信息等

信息。其中用户名和好友用户名共同为主键，好友用户名为作为外键，好友备注信息默认为用户昵称，好友信息表如表2.2所示。

表2.2 好友信息表

|  |  |  |  |
| --- | --- | --- | --- |
| 字段 | 字段类型 | 字段描述 | 备注 |
| F\_FID | Int | 好友ID | 主键1 |
| F\_UID | Int | 用户ID | 主键2，外键 |
| F\_NoteName | Varchar (20) | 备注 | 默认为昵称 |

2.2.2 数据库操作接口的规定

安全聊天工具中使用MySQL数据库，通过MySQL Dot Net驱动来连接数据库，并且在服务端系统启动后保持长连接。在服务端系统中通过自定义的MDO对象来操作数据库，使用驱动提供的基础方法封装后生成了更高级的数据库操作接口，提供给服务端与数据库的交互使用。接口规定了操作名称、参数列表、返回值、备注等信息，接口的详细信息如表2.3所示。

表2.3 数据库操作接口

|  |  |  |  |
| --- | --- | --- | --- |
| 操作名称 | 参数列表 | 返回值 | 备注 |
| Login | 用户名，密码 | 用户信息 | 失败返回null |
| GetFriendList | 用户名 | 好友信息数组 | 请求用户好友列表 |
| UpdateUser | 用户名、昵称、签名 | 影响行数 | 修改用户个人信息 |
| UpdateNote | 用户名、好友用户名、备注 | 影响行数 | 修改好友备注信息 |
| DeleteFriend | 用户名、好友用户名 | 影响行数 | 删除好友 |
| UpdatePw | 用户名、旧密码、新密码 | 影响行数 | 修改用户密码 |
| SearchFriend | 用户名 | 用户信息 | 查找好友信息 |
| AddFriend | 用户名、好友用户名、备注 | 影响行数 | 添加好友 |

2.3 应用层通信协议设计

2.3.1 起止符通信协议的设计

通信协议主要用于服务端与客户端之间的数据传递[4]。本系统中的协议是指服务端或者客户端将接受到的数据分割成一个个数据包的规范。而对于安全聊天工具来说，传输数据的特点是长度不固定但是一般不会超过100个字符，并且对于数据传输的稳定性和可靠性有很高的要求。下面本文分析几种常见的应用层通信协议的特点并选择最适合在安全聊天工具的开发中使用的通信协议。

常用的应用层通信协议有结束符协议、固定数量分隔符协议、固定请求大小协议、起止符协议、头部格式固定并且包含内容长度的协议等等[5]。下面针对每一种协议的特点做简要的说明。

1、固定数目分隔符协议。固定数目分隔符协议适用于不需要区分请求类型的系统，

固定请求大小协议的特点是每一个数据包都是由固定数目的数据组成，并且每一个数据都使用同一个分隔符来分割。但是在本系统中的数据数目不固定，那么固定分隔符协议显然不能满足需求。

2、结束符协议。结束符协议是通过固定结束符标记一个数据包，也就说在数据缓冲区中每次发现一个固定结束符就认为找到了一个完整的请求并取出。这样的协议可以应对变长的数据，但是当请求的数据中出现固定结束符的时候或者出现结束符丢失的时候，协议的就可能出现一直解析错误的现象，导致了协议的稳定性和可靠性相对较差。

3、头部格式固定并且包含内容长度的协议。头部格式固定并且包含内容长度的协议的数据可靠性较高，这种协议通过头部标记来区分消息的起始，在通过消息头中包含的数据长度来确定数据的剩余长度。不过由于头部长度固定，更适合传递数据较长的场景下。

4、起止符协议。起止符协议的特点是通过固定的头部和固定的尾部来标识一个数据包。有了头部和尾部的同时标记保证准确分割数据，这时可能出现一个问题是当传递的数据中出现系统规定的结尾标志时，会出现数据解析遗漏和解析错误的现象。当数据结尾出现重复的时候，可以根据找到了数据头部这一条件来辨识上一条数据出现丢失的情况，防止后面的数据的解析被干扰。

对于起止符协议是基本符合本系统的对数据传输的要求的。但是出现数据丢失的现象本系统中也是容忍度很低的。为了尽可能避免这样的数据丢失问题，我选择了8个字节的头部和8个字节的尾部，这种设计出现重复的概率是多少呢？下面的部分来进行一下论证。

由于每个字节有8个bit位，也就是说每个字节有256中选择，而8个字节就是256的8次方。换句话说，8个字节的固定头部与固定尾部有1/18446744073709551616的概括会出现与规定的头部或者结尾重复的现象。再假设一共有10000000的用户，每个用户平均每天3000条数据要传输，那么一年中出现重复的概率是1/18446744073709551616\*10000000\*3000\*365，这是一个小于0.01%的数字。这样的一个小概率事件，有理由相信是不可能发生的。

通过以上的论证证实，采用8个字节的头部和尾部的起止符协议是符合本文的预期设想的，满足了本系统中的短数据、不定长、不定参数的数据特点。

2.3.2 服务端与客户端之间通信接口的规定

基于上述固定起止符协议，服务端与客户端之间通信接口详细的规定了服务端发往客户端以及客户端发往服务端的数据包中的命令、数据项、数据项分隔符，如表2.1，表2.2所示。命令与数据项之间均是通过“：”来分割，数据项之间均是通过“，”来分割。如果数据项是一个完整的数据实体，就会使用json的类的序列化与反序列化的方法来将实体数据转换完json数组，作为一个整体作为数据项来传递[7]。

表2.3 客户端发送到服务端的数据接口说明

|  |  |  |
| --- | --- | --- |
| 命令 | 数据项 | 说明 |
| Login | 用户名，密码，私钥签名 | 登录 |
| AddFriend | 用户名，好友用户名，好友备注 | 添加好友 |
| DeleteFriend | 用户名，好友用户名 | 删除好友 |
| FriendList | 用户名 | 获取好友列表 |
| ReceiveMsg | 接收者，消息类型，消息 | 转发消息 |
| SearchFriend | 用户名 | 查找好友 |
| UpdateNote | 用户名，朋友的用户名，新备注 | 修改好友备注 |
| UpdatePw | 用户名，旧密码，新密码 | 修改登录密码 |
| UpdateUser | 用户名，昵称，签名 | 修改个人信息 |

表2.4 服务端发送到客户端的数据接口说明

|  |  |  |
| --- | --- | --- |
| 命令 | 数据项 | 说明 |
| FriendList | 好友列表的json串 | 好友列表的json形式 |
| Login | 登录结果 | 登陆者的信息，登录失败返回null |
| ReceiveMsg | 发送者，消息类型，消息 | 接收到好友消息 |
| SearchFriend | 查找到结果的json串 | 好友信息，未找到返回null |
| UpdatePw | 修改密码结果 | 修改密码是否成功的结果 |

2.4 服务端数据解析与分发设计

本系统的服务端使用基于Dot Net平台的SuperSocket开源框架来搭建[8]。SuperSocket是一个轻量级, 跨平台而且可扩展的Socket 服务器程序框架。基于SuperSocket框架，我定义了起止符协议来支持系统的通信架构和一个起止符协议制作工厂用来在SuperSocket中启动自定义的通信协议。

SuperSocket通过一个自定义的ChatServer类来管理服务端，控制服务端的启动、停止以及管理所有连接Session。每当一个客户端连接到服务端时，一个ChatSession就会被启动，这个Session的实例用来发送数据到对应的客户端，接受客户端发送的数据或者关闭当前连接，所有连接到服务端的Session都会被保存在ChatServer的Sessions池中。理论上说，可以使用通过Sessions池给任何连接到系统的客户端发送消息。

当服务端收到数据时，所有来自客户端的按照通信协议规定发送的请求都会被按照起止符协议的规定解析成自定义的ChatReceiveInfo数据包。这个数据包主要包括Key和Body两部分内容，Key代表本次请求的命令，Body代表本次请求的所携带的数据。SuperSocket通过Dot Net反射机制的查看自定义的命令类的类名并与ChatReceiveInfo数据包中Key字段做比较。当发现相同项时，就会生成对应的命令类的对象，并将数据包传到这个类的ExecuteCommand方法中，最后调用这个方法。此时，数据的解析和分发就已经完成，服务端根据对于请求命令的不同，使用传递进来的参数做出对应的业务逻辑处理和判断、数据的存取以及通过Session的id转发消息到对应的客户端。到此，服务端的数据解析与分发的设计就此完成。通过SuperSocket框架，系统实现了自定义的数据通信协议的制定以及对应的请求的分发和处理工作，并且可以很方便的完成通信协议的更换以及业务的扩展。

2.5 客户端的SuperClient框架设计

Socket是基于传输层通信协议封装的编程接口。通过一对已经建立连接的Socket应用程序，就可以互相发送消息和接受消息。在上一小节中，本文通过SuperSocket框架完成了服务端的设计工作，在本节中来阐述一下我自主的设计的客户端框架SuperClient。在服务端已经开启端口监听的基础，只要是按照服务端的IP地址和服务端监听的Port与其建立起Socket连接，客户端就可以与服务端交换通信数据了。但是在安全聊天工具中，需要较为复杂的业务判断，并且数据请求的种类较多，数据分发的目标也不能统一。基于这种情况，我设计了SuperClient框架来规范开发过程，简化客户端数据解析的流程。

2.5.1 SuperClient框架概述

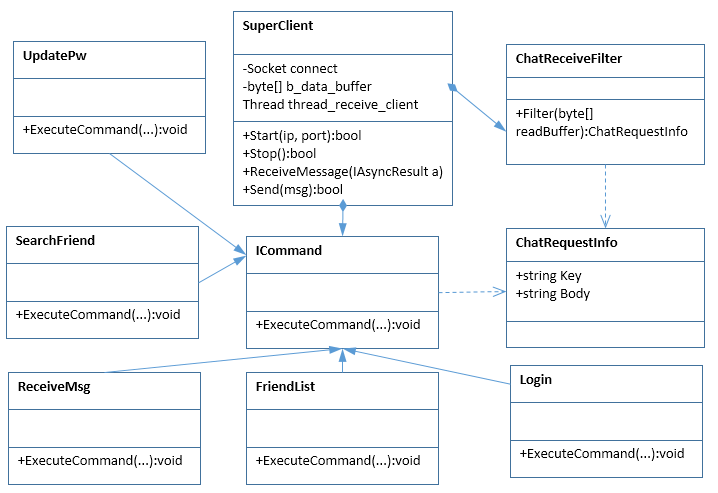
SuperClient框架是基于Socket网络通信编程接口，实现发送客户端请求、解析服务端数据以及数据分发的客户端通信框架。在本框架中，各个功能的控制都在核心类SuperClient中，每一个SuperClient的实例对应一个客户端。使用IP地址与Port作为参数调用对应的方法中就可以建立与服务端的连接，在SuperClient实例中，配置起止符通信协议和命令生成工厂，就可以接收并解析服务端发来的数据包。最后再根据解析出来的命令生成对应的命令的实体。由于所有的命令都继承自通过一个命令接口，根据面向对象中多态的特性，解析出来的数据可以动态的传递到命令的实体中。通过命令接口统一业务代码的业务执行方法，以此来减少业务代码的耦合度。SuperClient的类图如图2.1所示。

图2.1 SuperClient类图

这里简单的说明一下这个类图，然后在下面的2.4.2和2.4.3中会详细的介绍SuperClient的工作原理。SuperClient类是核心类，客户端的启动、停止、消息的接收和发送都在这个类中操作。ICommand类是所有命令类的父类，其他的命令类都要继承Icommand类并且实现抽象方法ExecuteCommand。ChatReceiveFilter类是负责数据解析，起止符通信协议就在这个类中实现，而解析后的数据包都会被实例化为ChatRequestInfo类。而ChatRequestInfo类作为ExecuteCommand方法的参数来使用。

2.5.2 SuperClient框架的使用方法

SuperClient框架设计的初衷就是让基于Socket的网络通信客户端的开发变得简单。有了它可以让开发者专注于业务逻辑的思考，在设计好应用层的通信协议后就可以轻松的开始业务代码的编写，让Socket客户端的开发变得快速。下面简单的介绍SuperClient的使用方法。

使用SuperClient进行数据通信是很简单的。SuperClient中使用SuperClient类来作为数据通信的核心类，每一个客户端对于一个SuperClient的实体。调用其Start方法和

Stop方法就可以启动和停止通信功能，使用Send方法，就可以实现消息的发送。而接受服务器发送的消息还需要做一点额外的工作。

在SuperClient中内置了起止符协议，在第2章中已经详细介绍了这个协议的特点，基本可以满足常规的开发需求，对于安全聊天工具来说也是非常好的选择。当有一类新的数据从服务端发过来的时候，开发人员只需要编写一个以命令为类名的Command类。这个类需要继承ICommand这个接口并实现其ExecuteCommand方法，在这个方法中就可以通过方法的参数获取到服务端发送的消息。

2.5.3 SuperClient的数据通信原理

熟悉开发框架的基本原理有利于更快的上手使用和开发过程中的bug的排除工作，下面来基于其数据通信的原理为核心，解释一下SuperClient的实现原理。

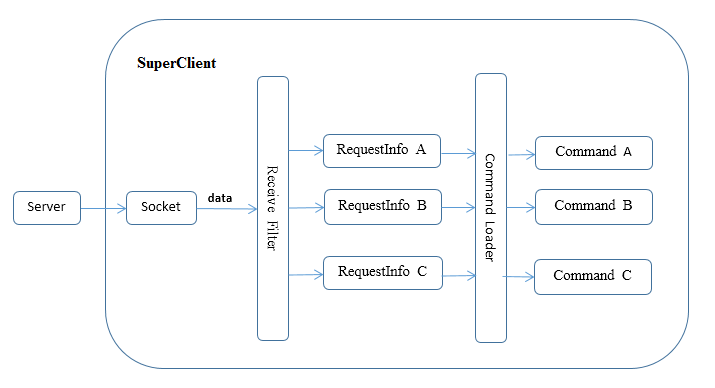
SuperClient是基于Socket网路编程接口实现的数据通信，这是通信原理的基础[9]。如图2.2所示，当SuperClient与服务器建立连接后，客户端收到的数据都会先缓存到消

图2.2 SuperClient 数据处理模型图

息数组中。框架内置的起止符协议会循环的从缓存中读取数据并从数据找到符合起止符协议规定的一条条完整的请求，每一个请求都会被实例化成ChatRequestInfo类型并返回给SuperClient命令加载器。而SuperClient通过反射的方式查找到哪些公开的类实现了基础的命令接口，进而帮助命令加载器找到与ChatRequestInfo实例的Key相同的类。这时，命令命令加载器就会生成了命令的实例，然后执行其ExecuteCommand方法，通过方法参数将服务端发送过来的数据传递到此命令的ExecuteCommand方法中。综上所述，SuperClient实现了将服务端发送过来的数据解析成规定的形式并且分发到相应的业务处理命令类中。

2.6 多线程通信

SuperClient框架实现了客户端的数据发送、接受、解析与分发的工作，其中数据的分发可以实现不同种类的数据分发到不同的命令类中处理。对于客户端与服务端通信这一类的较为耗时的操作是要在建立新的工作线程来完成的，但是从服务端接收的数据或者消息大多要在主线程中使用。所以，如何解决多线程间的数据通信就是下一个要阐明的问题。

对于安全聊天工具中的线程通信来说，数据流向都是从工作线程流往主线程。此外，在winform开发平台，主线程也同样是UI线程。所以，本系统中使用控件的Invoke方法通过委托的方式来完成工作线程到主线程的数据通信工作。Control的Invoke方法原理就是基于windows的消息系统，以消息的形式将数据从工作线程传递到主线程中。下面本文来具体说明一下如何使用Control的Invoke方法来完成数据的线程间传递[10]。

首先，要在主线程中建立委托，并且在UI初始化的同时使用UI线程中的数据操作方法来初始化委托。这样当委托被执行的时候，就可以将从服务端接受到的数据传递到UI线程中，在数据操作方法中完成相依的数据操作。然后，还需要在工作线程中调用控件的Invoke方法。当解析后的ChatRequestInfo数据包被分发到相对应的Command类中时，在ExecuteCommand方法中调用所需控件的Invoke方法，并按照参数列表来初始参数，指定UI线程的委托就会被执行。到此，这个线程间数据通信全部完成。

2.7 本章小结

本章主要讲述了安全聊天工具这个系统的全部数据通信结架构的设计工作。本系统中的主要包含服务端与数据库的数据交互，服务端与客户端的数据通信、客户端中还包含工作线程与主线程的线程间的数据通信。此外，本章还包含了系统的数据库设计、应用层通信协议的设计、服务端与客户端通信的命令接口的设计以及客户端通信架构SuperClient的设计。到此，本系统的所有数据传递线路全部打通。

# 第3章 安全性保证策略

对于安全聊天工具来说，安全性能是评估软件好与坏的核心标准。所以在本章着重解释安全聊天工具使用了哪些安全策略来保障用户的通信数据的安全的。本系统的安全性的保障主要是从两个角度来实现，第一、尽最大可能降低用户数据被泄漏的风险；第二、当用户数据被泄露时，也要保证用户隐私安全。针对以上两点，本系统使用了基于RSA加密算法的通信数据加密策略、基于用户口令+实体token的身份验证增强策略、阅后即焚安全策略以及SQL注入防御策略等多角度、全方面的安全策略来保证用户数据的安全性。下面几个小节针对这些安全性保证策略做详细的解释和说明。

3.1 数据加密传输策略

3.1.1 加密算法的选择

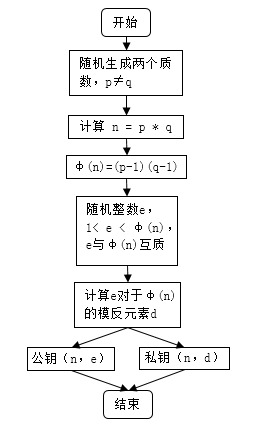
关于加密算法，主要分为对称加密算法和非对称加密算法两大类。对称加密算法中，信息的加密和解密使用的都是同一个密钥。这要一来，数据的发送者的密钥需要使用某种方式来来传递给接受者。这对于安全聊天工具来说，就意味着任何一个消息的接受者都可以获取到发送者的密钥，这对数据的安全性产生了很大的威胁，而非对称加密算法很好的解决了这个问题。

非对称加密算法采用两个相互依赖的密钥，消息发送者使用公钥对消息进行加密，公钥公开，可以在根据需要获取。而私钥保密，不会公开。消息的发送者使用消息接受者的公钥来加密数据，消息接受者使用自己私钥解密发送给自己的消息，这样就极大的降低了密钥泄漏的风险，提高了用户数据的安全性。由此可见，非对称加密算法更适合于对安全性要求较高的即时通讯工具。在非对称加密算法中，应用最广泛的就是RSA加密算法，在下一部分将着重解释RSA非对称加密算法的原理和使用在安全聊天工具中的具体应用方法。

3.1.2 RSA加密算法的基本原理

RSA加密算法是目前最有影响力的非对称加密算法，它能够抵抗到目前为止已知的绝大多数密码攻击。RSA算法的核心是基于一个简单的数论事实，那就是两个大质数的乘积的因式分解极为困难[11]。下面本文详细分析一下RSA算法的密钥生成、公钥加密、私钥解密的过程，在讲述的过程中涉及的数学原理不做过多的解释。

先分析一下密钥的生成过程，如图3.1所示。首选随机选择两个不相等的质数p和q，计算p和q的乘积得到n。然后计算n的欧拉函数φ(n)，φ(n)的值为q-1与p-1的乘积。之后再随机选择一个整数e，条件是1< e < φ(n)，且e与φ(n) 互质。最后在计算e对于φ(n)的模反元素d，密钥生成的过程就完成了。由n和e组成公钥，n和d组成私钥。

图3.1 RSA密钥生成流程图

有了公钥和私钥就可以开始数据的加密和解密任务。假设需要加密的信息m，使用公钥 (n,e) 对m进行加密。这里需要注意，m必须是整数（字符串可以取ascii值或unicode值），且m必须小于n。那么，加密后的数据c ≡ me (mod n)。解密数据的过程类似，使用私钥 (n,d) 来解密，解密的过程为m ≡ cd (mod n)。这样，数据m加密和解密的过程就解释完成。

通过上面的过程，对RSA算法加密的过程有了基本的了解。基于RSA算法的密钥生成、加密解密过程，下面分析一下RSA算法的可靠性。在公钥与私钥的生成过程中一共出现了p、q、n、φ(n)、e、d这6个数字。这六个数字之中，公钥用到了两个（n和e），其余四个数字都是不公开的。其中最关键的是d，因为n和d组成了私钥，一旦d泄漏，就等于私钥泄漏。

现在已知公钥 (n,e) 的条件下，按照密钥的生成过程逆向计算私钥 (n,d) 中d数字。ed≡1 (mod φ(n))。只有知道e和φ(n)，才能算出d。e是在公钥中已知的数字，而φ(n)=(p-1)(q-1)。只有知道p和q，才能算出φ(n)。最后，n = pq。只有将n因数分解，才能算出p和q。如果n可以被因数分解，d就可以算出，也就意味着私钥被破解。可是，大整数的因数分解，是一件非常困难的事情。目前，除了暴力破解，还没有发现别的有效方法。在维基百科中有如下记录[12]，"对极大整数做因数分解的难度决定了RSA算法的可靠性。换言之，对一极大整数做因数分解愈困难，RSA算法愈可靠。假如有人找到一种快速因数分解的算法，那么RSA的可靠性就会极度下降。但找到这样的算法的可能性是非常小的。今天只有短的RSA密钥才可能被暴力破解。到2016年为止，世界上还没有任何可靠的攻击RSA算法的方式。只要密钥长度足够长，用RSA加密的信息实际上是不能被解破的。"

基于以上分析证明，在安全聊天工具中使用RSA加密算法可以保证数据即使被截获的情况也能极大的提升数据的安全性。在私钥没有泄露且使用了足够长的密匙的条件下，用户的数据被破解的可能极低的。

3.1.3 公钥与私钥在系统中的应用

在了解了RSA加密算法的原理之后，下面阐述一下如何在安全聊天工具系统中使用RSA加密来保证用户数据安全。

由于RSA算法中私钥的重要程度，所以有必要说明一下在本系统中的密钥的生成的过程。为了避免私钥的泄露，当私钥生成之后，严格禁止通过网络的方式来将私钥交到用户手中。基于这一点要求，有两个方案来生成密钥。

第一种方案是在客户端生成密钥。由于公钥是可以公开出去的，所以在客户端生成密钥之后可以通过网络将公钥传递到服务端保存好，待有需要时通过网络获取即可。但是这样的缺点就是用户在更换pc机后无法获取自己的私钥，这样也就无法解密发送给自己的数据。第二种方案是当用户发出注册请求时，在服务器生成密钥如图3.2所示。将公钥直接保存在服务端的数据库中，将私钥直接在服务端通过外部生产环境制作成实体的token，然后在通过现实环境将私钥以实体token的形式交到用户手中。这样的方式虽然会在注册和用户使用时造成一些时间上的延长，但是带来的好处也是巨大的。有了实体token的存在，用户就可以在任意安装了安全聊天工具客户端的pc机上使用自己的帐号来完成即时通讯。更重要的是，用户数据的安全性得到极大的提升。所以，本系统采用第二种方法来生成密钥。

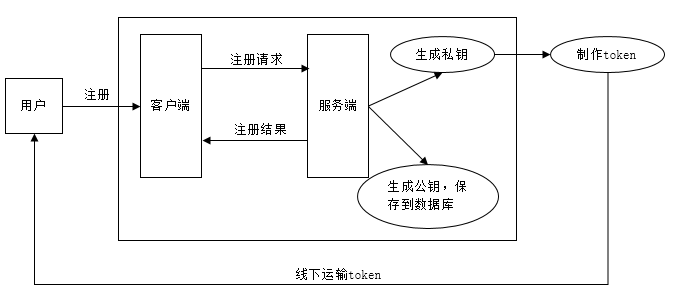
有了密钥再说明一下用户加密和解密数据的过程，这里对RSA加密算法做了一个小的改进，本系统中除了对聊天消息进行数据加密外，还使用数字签名的方法来验证数据是否从预期的发送者发送过来，下面来具体解释一下加密解密的过程。来当用户需要给自己的某一个好友发送消息时，首先使用自己的私钥加密自己的用户名，然后将密文与要发送的数据一起按照通讯协议来打包。而客户端会直接向服务端请求此好友的公钥，使用好友的公钥将要发送的数据与私钥加密后的用户名一起加密，然后打包发送给好友。服务端收到用户发送的聊天信息会直接根据信息接受者转发此数据包，当指定的好友收

图3.2 密钥生成模型图

到消息后，首先使用自己的私钥将消息第一次解密，通过解密可以获取到消息的发送者，消息类型以及通过签名加密过数据。然后再向服务端请求消息发送者的公钥来解密这个签名后的数据，如果解密出来的用户名与发送者的用户名相同，此消息才是有效消息并传递到主线程；如果不相同则舍弃消息并向用户和服务端报警，提示有恶意的攻击行为发生。到此，安全聊天工具通过数据的加密解密的方式来保证数据安全的过程全部解释完成。有了私钥来保证消息发送的消息即时被截获，在没有私钥的情况下也无法获取消息内容；而有了消息签名又可以保证接受到的消息来自正确的发送方，保护用户不被欺骗。通过这样的数据加密传输策略可以有效的降低用户数据泄露的风险。

3.2 身份验证增强策略

比较常见的用户身份验证策略是使用“用户名+用户口令”的方式，用户进行身份验证时，只需要输入自己用户名和密码，由客户端向服务端发出验证请求。然后通过比较用户输入与数据库中数据来返回结果，如果正确用户身份验证成功，允许下一步操作。如果身份验证失败，则会阻止用户的登录系统。这样的策略的风险就是当用户的口令泄露时，如果用户不能第一时间发现并更改密码，用户的数据安全就面临这极大的威胁。为了降低这样的风险，本系统在原有的“用户名+用户口令”的身份验证策略的基础上，增加了“签名验证”的策略来进一步提高身份验证的安全系数。

在安全聊天工具的系统中，使用的身份验证的流程如图3.3所示。用户在客户端输入用户名、密码的同时，还要求用户在pc机上使用自己的私钥。当用户发出身份验证的请求时，客户端使用本地的私钥加密用户名，然后将用户名、密码、加密后的签名信息一同发送给给服务器，并且请求验证用户身份，当客户端在本地无法检测到实体token中的私钥的时候，系统会拒绝用户的身份验证请求。服务端监听到客户端的请求后，先根据第一个用户名从数据库中找到用户的公钥，然后使用公钥将签名信息解密。将解密结果与第一个用户名做比较，如果比较结果不相同，则会客户端向发消息提示用户token与用户名不对应；如果相同再比较用户密码是否正确，再将验证结果返回给客户端，客户端接收到用户身份验证成功的消息才会允许用户的进一步操作，这就是一个完整的用户身份验证的过程。

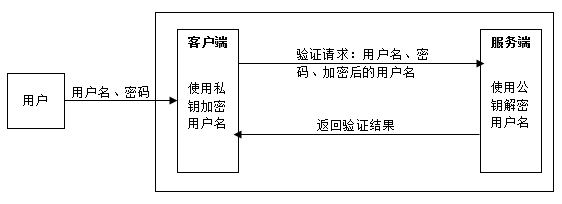
在安全聊天工具中，通过“用户名+用户口令+用户签名”的多重身份验证的保护策略下，即使发生用户口令泄露这样的事件，也有用户签名验证这样的安全策略来保障用户的个人信息的安全。让恶意得到用户名和用户登录口令的人在没有token的情况下也无法窃取用户信息。

图3.3 用户身份验证模型图

* 1. SQL注入防御策略

SQL注入是一种常见服务器攻击方式，攻击者在系统的输入域中插入恶意的SQL语句，欺骗服务端进行错误的操作，这样可能导致数据库的数据安全遭到威胁，用户的个人信息有泄漏的风险。对于SQL注入，必须采取相应的防御策略来保证安全聊天工具的服务端的正常运行。下面先说明SQL注入的基本原理，在详细解释防御SQL注入的两种常用的策略。

* + 1. SQL注入的基本原理

当服务端想要获取数据库中一些特定的数据时，基本的流程是先连接数据库，再按照SQL语法规定以及获取数据的特点编写核实的SQL语句，在根据返回的结果集做相应的操作。在开发过程中，最容易出现风险的位置就是根据查询数据的特点构造符合mysql需要的SQL语句[13]。当SQL语句还需要用户输入的一些信息来辅助查询的时候，这时候就存在一种风险，下面通过一个例子来简单说明这种风险。

假设在系统的数据库有一张User（id， name）表，User表的结构比较简单，只有id和name两个字段。当用户需要查询用户id为1001的用户的name的时候，通过会写出这样的一条SQL语句：SELECT name FROM User WHERE id = ‘1001’，这时候id这个数据1001一般是由用户输入的。在理想的情况下，用户输入id号，服务端构造SQL语句，到数据库中执行，然后取回name结果返回给用户，整个流程完成。但是，如果用户输入的id并不是系统预期的数字，而是“1001’ or ‘1’ = 1”的数据，服务端的整个SQL语句变成了这样：SELECT name FROM User WHERE id = ‘1001’ or ‘1’ = 1。显而易见的是，不论用户输入的id数字是否在数据库中存在，都会因为or 后面的语句导致WHERE语句恒成立，这样就可以取到数据库表中所有的用户的用户名。这虽然只是一个很简单例子，但是SQL注入攻击的威力可见一斑。如果攻击者在用户输入域中输入更复杂的查询语句，就会导致更严重的数据泄露、数据丢失等严重威胁。所以，安全聊天工具必须采取相应的策略来防御SQL注入的攻击。在安全聊天工具的开发中，共采用了两种安全策略来防御SQL注入的攻击，具体的防御方式，将在下面的两个部分做详细的解释。

* + 1. 关键词过滤

为了应对SQL注入的攻击，本系统采用的第一种防御策略是关键词过滤。在SQL注入的基本原理的讲解部分中提到，SQL注入都是从攻击者的非法输入开始的。而一般需要通过输入一些关键词、特殊符号等语句来完成完成SQL注入攻击。所以，本文从这个基本点入手，通过关键词过滤的角度来防御SQL注入攻击[14]。

本系统的关键词过滤工作主要集中在客户端进行，在收集用户的输入信息后，首先使用关键词过滤组件将输入中出现的“SELECT、UPDATE、INSERT、DELETE、AND、OR、分号、注释符号”等等在SQL语法中可能使用的关键词以及符号全部删除。将攻击者输入的信息过滤掉特殊的关键词后再代入SQL语句中使用，这样就从一定程度上降低了被SQL注入攻击的风险。

* + 1. 参数绑定

在关键词过滤的安全策略中，可能会出现关键词遗漏或者攻击者避开输入关键词的方式的来攻击系统，如果，攻击者可能将SQL注入的语句转换为16进制的字符输入进系统，这时候关键词过滤的保护策略就会出现失效的风险，仅仅通过这样一种策略并不能很好的防御SQL的攻击。为了应对这种逃避关键词过滤的攻击方式，本系统使用了另种更巧妙的防御策略，参数绑定安全策略。

这是一种通过SQL语句的参数绑定的方式来防御SQL注入的安全策略。在解释SQL的基本原理的部分时，本文提到了一个User表的例子。在那个例子中使用的SQL语句是：SELECT name FROM User WHERE id = ‘1001’。其中预期的参数只有id一个，这条语句的含义是找到用户id是1001的用户的名字。但是，在SQL注入攻击时，语句是：SELECT name FROM User WHERE id = ‘1001’ or ‘1’ = 1。输入的参数并没有全部作为id来使用，而是因为输入的特殊性改变了原本SQL语句的含义。这条语句的含义变成了返回User表中所有用户的名字，条件部分因为输入全部失效了。由此可以看出，攻击者攻击的实质是通过输入精心设计的SQL语句来改变原来SQL语句含义，以达到破坏系统或者窃取用户信息的目的。所以，针对这样的情况，本系统通过一定的技术手段来保护SQL语句的含义不被攻击者通过注入的手段篡改。对应上面的例子来说，如果客户端可以将攻击者输入的全部内容作为‘id’来执行SQL语句，那么结果就会跟系统预期的保持一致了。按照这样的想法，参数绑定后的的SQL语句变成了下面的样子：SELECT name FROM User WHERE id = ‘(1001’ or ‘1’ = 1’ )’。解释出来就是：找到User表中id是 (1001’ or ‘1’ = 1) 的用户的name。显然这个用户id是不存在的，也就查询不到name的结果集。这样也就成功的防御了SQL注入攻击，这种参数绑定的安全策略是有效的。在mysql for dot net的驱动中提供了MySqlCommand类中的Parameters方法来实现SQL语句参数的绑定功能，用户输入的参数只能被固定的参数替换，这样就实现了上面叙述的效果。

* 1. 阅后即焚安全策略

以上都是从技术的层面来实现安全性能的保证，本模块安全聊天工具从功能的角度来进一步增强系统的安全性。在安全聊天工具中提供了“阅后即焚”的特色功能，来让用户的信息的保密级别再次升级。如果用户通过本系统与好友交流的信息对保密性要求极高，达到了最好只让对方看几秒钟就从系统中消失的层次，那么便可以使用“阅后即焚”的安全策略。

阅后即焚功能是指，当用户启动阅后即焚的功能后，发送的消息的消息类型会被标记为“阅焚消息”，传递到好友客户端的阅焚消息会被特殊的处理。具体体现在好友接收到消息后，不是直接就可以看见消息的内容，而是需要主动点击消息触发查看事件后，才能查看消息。更重要的是被设置为阅后即焚的消息只会显示一定的时间就会被销毁，显示的时间是会根据消息的长度，按照1秒/10字的速度来计算。当消息被销毁后，用户没有任何办法从系统中再次查看此消息的具体内容。通过这样的功能，用户可以根据自身的情况，自主的选择是否启动阅后即焚的消息。有了阅后即焚的功能，用户数据的安全性再次升级。

* 1. 本章小结

安全是安全聊天工具设计与实现的核心，也是衡量本系统的好坏的关键性指标。在安全聊天工具中，以RSA加密算法为核心，以阅后即焚的功能角度安全策略为亮点，从用户身份验证的用户名签名技术，到用户数据传输的公钥加密、私钥加密、数据签名验证，再到SQL注入防御策略这一系列的安全性保证策略来全方位的保证用户的个人信息和即时通信消息的安全。各个防御策略各司其职又互有交叉，当用户个人原因导致少量关键验证信息泄露或者系统遭到恶意攻击时，这些防御策略也能极大的保护用户隐私不受到侵害。

# 第4章 安全聊天工具的详细设计与实现

到了这一章，整个系统的数据通信线路已经全部打通，作为核心的安全性保证策略也已经全部完工，相当于整个系统的脚手架和一些必要的功能模块全部准备就绪，在本章就要将这些模块都组装起来并且要完成很多细节的设计和实现的工作。所以，本章主要从安全聊天工具的各个功能模块的角度，依托于前两章的内容完成系统的详细设计和实现的部分。

4.1 系统功能模块的设计与实现

4.1.1 初始化模块

当安全聊天工具的客户端启动的同时，也会启动SuperClient调用Start方法来尝试连接指定的服务端。当连接失败时会提示“请检查网络连接”，如图4.1所示。点击确定后，客户端会自动退出。当网络环境恢复正常后，用户可以尝试再次启动客户端。此外，客户端还会检查当前的pc环境中是否包含有官方制作的包含用户信息和私钥的token，只有客户端检查到合法的token的存在的时候，用户才有登录系统的权利。当客户端成功连接到服务端时，客户端会正常加载登录界面。此时，在系统内部的SuperClient会启动工作线程，等待处理服务端发送过来的消息。

图4.1 网络连接失败

4.1.2 身份验证模块

身份验证使用安全性保证的第一道关卡，当用户打开系统的客户端的时候，需要在PC机上插入带有自己私钥的实体token，再填入用户名和密码，最后点击登录按钮即可向服务端发出身份验证请求，按照第3章第2小节中讲述的身份验证增强策略来验证用户身份，用户的登录窗口如图4.2所示。客户端会调用SuperClient的Send方法将验证信息发送到服务器并请求身份验证。服务端收到客户端的身份验证的请求后，会验证用户的用户名、用户口令以及用户签名信息是否正确，验证完成后再讲结果反馈给客户端。当客户端接受到服务端的反馈结果的时候，如果登录成功则隐藏当前登录窗口并加载用户主控制面板，然后向服务端请求用户的好友列表以及将用户的个人信息传递到当前面板中并显示，如果登录失败则获得提示信息，用户可以根据反馈信息修改验证信息或者更换token。

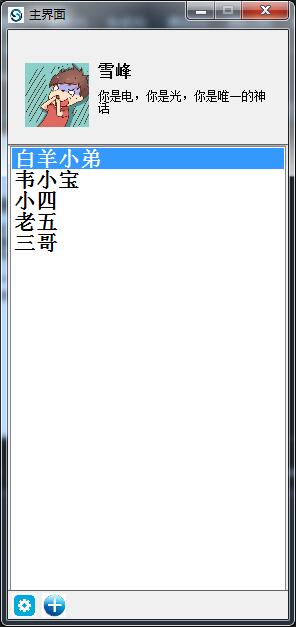
图4.2 用户身份验证界面

4.1.3 消息通信模块

当用户登陆成功后，客户端会调用SuperClient向服务端请求用户的好友列表，当服务端收到请求好友列表命令的时候会从数据库中读取该用户的好友信息，并使用类的序列化方法将好友信息的转成json数组的形式返回到客户端。当客户端收到反馈后，再使用类的反序列化的方式将json数组转成好友信息的对象的形式并显示到用户主控制面板上，如图4.3所示。

当需要发送消息给好友的时候，选中要发送消息的好友，通过双击或者右键选择“发送即时消息”的选项就可以打开与好友进行即时通信的窗口了，如图4.4所示。在聊天窗口的设计类中包含一个静态的用来保存已经打开的好友窗口的Hash集合，这个集合使用好友用户名作为键值，使用好友聊天的窗口的对象作为元素[15]。每当一个聊天窗口被打开时，系统都会检查Hash集合中是否包含以此好友为键值的元素来确定此好友聊天窗口是不是已经被打开，如果已经被打开则会激活原窗口；如果没有被打开则会初始化一个新的聊天窗口并加入到Hash集合中。

当聊天窗口加载完成后，就可以在下面的输入区中编辑想要发送的消息，点击发送

图4.3 用户主控制面板

按钮或者按“ENTER”键就可以发送消息到好友的客户端。这里有两种发送模式供用户选择，第一种是普通模式，第二种是阅后即焚模式。这两种模式通过取消和选中“阅后即焚”的复选框来控制，也可以使用快捷键“Ctrl + Y”来选择。关于阅后即焚的功能的介绍在第3章第4小节已经有了详细的说明，这里不在赘述。

当用户发送消息后，客户端会先检查检查用户输入是否为空。当用户输入为空时，系统会给予提示，并阻止空消息的发送。在输入检查完成之后，客户端会将用户准备发送的消息加密，然后再将好友的用户名、加密后的消息、消息类型按照通信协议的要求封装好，再发送到服务端，而服务端接到即时通信类的消息时，并不会解析和解密用户

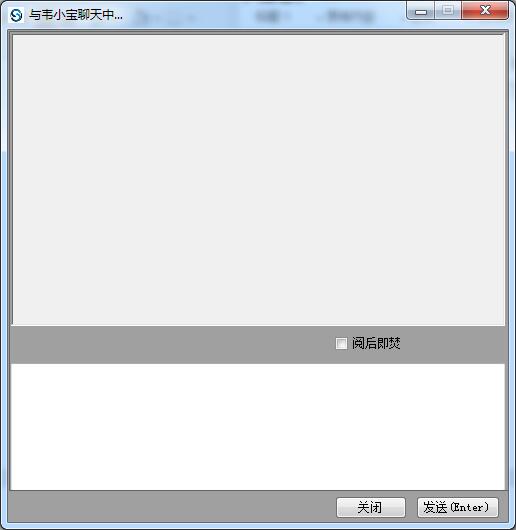
发送的消息的内容，只是根据消息接受者的用户名来转发消息到相应的好友的客户端。当消息成功发送到客户端后，用户发送的消息会显示在聊天窗口上半部分的消息显示区域。如果用户发送的消息是阅后即焚的消息类型，则只会显示“阅后即焚”，不显示具体的消息内容。

图4.4 通信窗口图

当用户收到好友发送的消息时，首先会由命令加载器来分发消息到用户主控制面板的好友消息分发器，由好友消息分发器解析出消息的发送者、消息类型以及加密后的消息主体。然后好友消息分发器会遍历用户的好友列表，找到对应消息发送者的信息来初始化或者激活一个聊天窗体，并将消息的发送者、消息类型以及加密后的消息主体转发到此好友的消息显示器中处理。在消息显示器中，客户端按照解密策略来解密数据并显示到消息显示区域。当消息是阅后即焚类型的时候，消息显示器会先将消息连同消息所在行一同存储在消息集合中，然后会先显示为红色字体的“点击查看”字样。当用点击消息后，会从消息集合中取出消息并显示相应消息若干秒后，彻底销毁消息。

对于用户点击阅后即焚的消息时，有如下的逻辑判断。当用户点击消息显示区域的时候，客户端会判断用户所点击位置所在行的文字是否为红色字体的“点击查看”字样，如果不满足上述要求，系统则忽略本次点击事件；如果满足要求，则会根据点击位置所在行到消息集合中取出阅后即焚消息并显示。

4.1.4 用户信息管理模块

用户信息的管理主要包括用户个人信息的查看、更新、用户密码修改等功能，下面针对着几个功能的实现做详细的说明。

个人信息的查看与更新功能。当客户端发出身份验证的请求后，如果身份验证通过，服务端会返回用户的用户名、用户昵称以及个人签名等信息，再通过窗体间传递参数的方式将用户的基本信息发送到消息用户主控制面板并显示到个人信息的位置。同时，客户端中会在本次登录过程中保存用户的登陆状态和个人信息，为其他模块的使用做准备。当用户发出更新个人信息的请求时，客户端会加载个人信息修改面板，如图4.5所示。客户端会在个人信息修改面板中显示用户当前的个人信息的内容，以方便用户修改。可以修改的个人信息包括用户昵称和用户的个性签名。用户修改完成后点击确认按钮，此时客户端会将用户更新后的个人信息按照通信协议来打包并发送到服务端。在服务端来更换用户提供的用户名来定位用户并且将新的用户昵称和用户的个性签名写入到数据库用户信息表中，然后服务端会将数据更新的结果返回到客户端。当客户端收到服务端反馈更新成功后，会将个人信息修改面板关闭并提示用户更新成功，然后在更新用户主控制面板显示的用户信息，更新当前在系统中保存的用户个人信息；当客户端收到服务端反馈更新失败时，服务端会提示用户更新失败以及失败的原因，并允许用户重新修改个人信息

图4.5 个人信息修改

密码修改功能。密码的修改涉及到安全口令的保密问题，所以不能类似基础的个人信息修改一样，在用户登录的状态下就直接允许用户修改登录密码，需要增加身份验证的检验条件，具体过程如下。当用户发出密码修改的请求时，客户端会加载密码修改面板，如图4.6所示。用户需要输入当前登录密码、新密码、确认新密码三条数据。当用户点击确认按钮的时候，首先客户端会对新密码与确认新密码进行比较。如果新密码与确认新密码不一致，会提示用户重新输入新密码；如果比较结果一致的话，则由客户端使用本地私钥签名原密码，然后将用户名、签名后的密码，新密码打包并按照通信协议的规定发送的服务端做验证和修改。当服务端收到客户端修改密码的请求的时候，会先解密用户的原密码并与数据库中的数据比对，比对成功后才会将新密码写入到数据库中。如果比较结果失败，会将结果反馈到客户端。关于签名技术在本文的第3章第1节中的公钥与私钥在系统中的应用模块已经有了详细的解释和说明，这里不在赘述。在修改密码的过程中，身份验证通过了用户口令和私钥加密两种方式的验证，体现了本文对于用户安全性的多重保障。也同时因为包含私钥的实体token的存在，让用户将自己的个人信息牢牢的抓在自己的手中。

图4.6 修改密码

4.1.5 好友管理模块

好友管理模块实现了用户对于好友的的管理功能，具体包括好友查看、备注更新、好友添加、好友删除等功能，而好友管理是安全聊天工具的即时通信的基础之一，想要发送即时消息的双方要在添加成为好友的基础上才能成功。下面针对这些功能的详细设计和实现做进一步的解释和说明。

好友查看功能主要体现在用户登录成功后的好友列表加载。当用户登陆到安全聊天工具后，客户端会调用SuperClient向服务端请求用户的好友列表，当服务端收到请求好友列表命令的时候会从数据库中读取该用户的好友信息，并使用类的序列化方法将好友信息的转成json数组的形式返回到客户端。当客户端收到反馈后，再使用类的反序列化的方式将json数组转成好友信息的对象形式并显示到用户主控制面板上

好友备注更新功能的实现。当用户需要发出更新好友备注的请求时，客户端会加载好友备注修改面板，如4.7所示。此时用户可以输入新的好友备注信息，点击确认按钮。客户端会直接将用户名、好友用户名、好友新的备注信息发送到服务端。当服务端接受到修改好友信息的请求的时候，会将用户好友新的备注信息写入到数据库中，并将更新数据库的结果反馈给客户端。客户端根据服务端反馈的消息基于用户更新结果，关闭好友备注更新面板，并且刷新好友列表以保持当前好友列表与数据库数据的一致性。

图4.7 好友备注修改

好友的添加功能。在安全聊天工具的设计中，要求添加好友必须有好友准确的用户名，不提供模糊查找和条件查找的功能。这也是保护用户信息安全的一种手段，即用户不会在自己不知情的情况下被请求好友，只有用户主动在现实场景下交换用户名，才可以使用添加好友的功能。当用户想客户端发出添加好友的请求后，客户端会加载添加好友面板，如图4.8所示。用户需要输入完成在好友用户名才能找到对应好友信息，在核对好友信息准确无误后，用户点击添加按钮想客户端发出添加此好友的请求。客户端首先会先在用户的好友列表中查找此好友是否已经存在，如果已经添加过此好友，系统会提使用用户“ta已经是你的好友啦”，如图4.9所示。如果在好友列表中没有找到此好友，则会想服务端发起添加好友的请求。当想要添加的好友用户确认后才会被系统添加到好友列表中。

图4.8 添加好友

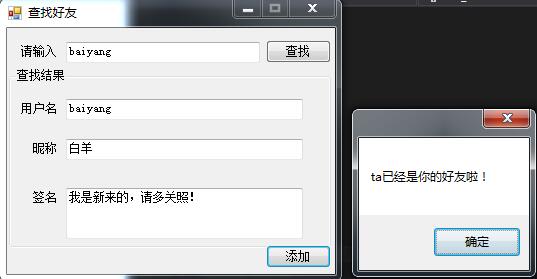
好友的删除功能。当用户发出“删除好友”的请求时，客户端会首先确认用户是否是误操作。当得到用户的确认删除答复后，客户端会将用户名、好友用户名打包发送的服务端请求删除此好友。当服务端收到删除请求后，会到数据库中从这个用户的好友列表中删除此好友，再将删除的结果返回给客户端的。客户端收到删除结果会判断，当删除成功时，提示用户“此好友删除成功”，并且刷新用户主控制面板中的好友列表以及在

图4.9 重复添加好友

SuperClient中的好友信息集合；如果删除失败时，客户端会提示用户删除失败以及原因，并允许用户重新操作删除好友。

4.2 系统安全性能测试

对于安全聊天工具的各种功能实现效果在上一小节的讲述已经有充足的说明，座椅本模块不再对功能才测试做详细的描述。而本文第3章中提到，安全性能是评价安全聊天工具好坏的核心标准[16]。所以，本章主要针对系统提出的四种安全性保证策略做充分的安全性能测试。

4.2.1 数据加密传输测试

数据加密传输的策略主要是保证数据在传递过程中被截获时不被攻击者获取到数据内容。所以，本测试通过vs2013开发攻击的debug功能来模拟攻击者截获到数据。通过数据监控来查看截获到数据的效果。

通过测试来模拟用户发送消息给好友的场景，如图4.10所示。当客户端发送的消息被截获到时，只能获得加密后的数据且无法通过此数据判断出消息原文。

图4.10 加密数据

4.2.2 身份验证测试

身份验证增强策略的方法是通过增加用户签名的方式来曾加身份验证的条件。当用户输入错误的用户名或者密码时，客户端提示用户密码或者用户名错误，如图4.11所示。当用户输入的正确的用户名和密码，但是本地的token不匹配时，客户端提示用户他本体token不匹配，如图4.12所示。当用户输入了正确的用户名和密码并且token匹配成功的时候，则可以登录客户端进行下一步操作。

图4.11 口令错误

图4.12 token不匹配

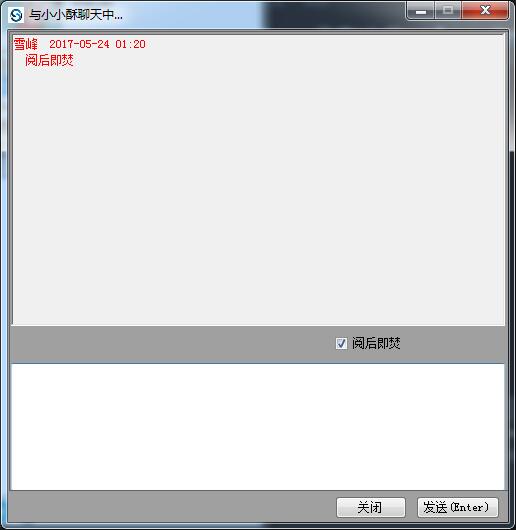
4.2.3 SQL注入防御测试

SQL注入的防御策略是防御攻击者通过输入域注入恶意的SQL语句攻击系统。当在登录时输入带有关键字的信息并提交的时候，系统提示不能输入非法字符，如图4.13所示。

4.2.4 阅后即焚功能测试

阅后即焚是本系统的特色功能，当用户给好友发送消息的时候可以选择开启或者关闭阅后即焚的功能。当用户在开启此功能的时候给好友发消息的时候，在自己的消息显示区域显示的是红色字体的“阅后即焚”的字样，而不是刚才原消息，如图4.14所示。

图4.13 非法输入拦截

当好友收到阅后即焚的消息的时候，显示的是红色字体的“点击查看”字样，如图4.15所示。当用户点击“点击查看”的时候，系统会提取消息队列中消息并显示，如图4.16所示。消息显示几秒后彻底删除消息，并显示绿色字体的“阅后即焚”，如图4.17所示。

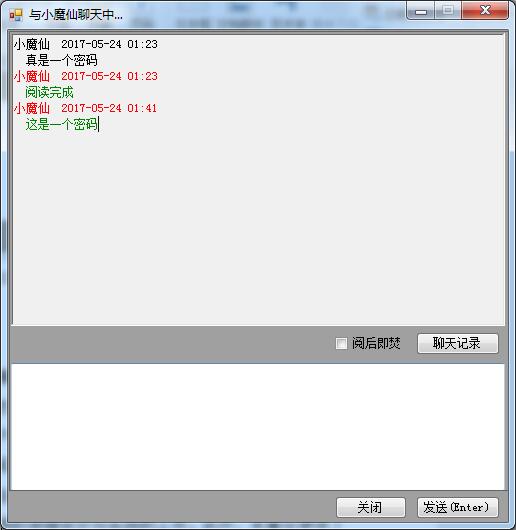
图4.14 发送阅焚消息

图4.15 收到阅焚消息

图4.16 查看阅焚消息图

4.17 销毁阅焚消息

4.3 本章小结

本章讲述了安全聊天工具的所有模块的详细设计和实现，是系统通信架构的设计和安全性保证策略的详细应用。在系统的各个功能模块的开发中，系统的通信架构就贯穿始终的，几乎所有的操作都是基于用户到客户端、客户端到服务端、服务端到数据库的通信结构的设计。而包括身份验证、阅后即焚的消息的发送与接收、用户密码的修改等等重要操作的进行都是基于第3章安全性保护策略的基础上的。在本章中，将所有功能的细节全部解释清楚，完成了整个系统的详细设计与实现的工作。此外，本章还讲述了系统的测试的相关工作，从功能测试和性能测试两个方面，体现了系统功能的可用性和安全的多重保障。

结　　论

安全性能性能是评价安全聊天工具的核心标准，在这个人人重视个人隐私的时代，提高即时通讯软件的安全性能更是重中之重。本文以RSA加密算法为核心，使用数据加密传输、身份验证增强、SQL防注入、阅后即焚这四种安全策略层层防护，有效的降低用户个人信息被泄露的风险。本系统使用SuperSocket框架、起止符通信协议以及SuperClient框架等技术，设计并实现了可以极大提升用户信息安全性的安全聊天工具。

本文所做的研究工作总结如下：

1、对即时通信类软件的的安全性的国内外研究现状进行了探索，对论文的主要内容和组织结构进行梳理和分析。

2、对安全聊天工具的所有模块的通信架构进行分析和解释。

3、着重对本系统中使用的各种安全策略的原理和具体应用进行分析和阐述

4、针对安全聊天工具的所有功能模块做详细设计和实现，将通信架构和安全保证策略应用到具体的功能中，并对系统的功能做了安全性能方面的测试。

综上所述，本文以安全保证为核心，设计并实现了一款基于RSA加密算法的安全聊天工具，并完成了一定的安全测试。测试结果显示，系统极大的降低了用户信息泄露的风险，达到预期效果。但是系统共仍有不足之处，如系统的功能与常用的即时通信工具相比较少，还有待完善。

参考文献

[1] 李勤.详解NSA “永恒之蓝”勒索蠕虫爆发，开机即可被勒索到底怎么回事[EB]. http://www.leiphone.com/news/201705/iGXUMArn1cP1livY.html, 2017-05-13.

[2] 凤凰科技.独立机构评测聊天软件安全性：QQ得零分安全性最差[EB]. http://tech.ifeng.com/a/20141105/40858846\_0.shtml,2014-11--05.

[3] 欧军. 基于socket的网络通信技术研究[D].成都:四川大学,2013.

[4] 王达.深入理解计算机网络[M].北京:中国水利水电出版社,2017:25-30.

[5] 江振宇. 内置的常用协议实现模版[CP]. http://docs.supersocket.net/v1-6/zh-CN/The-Built-in-Common-Format-Protocol-Implementation-Templates,2017-5-15.

[7] MSDN. 如何对 JSON 数据进行序列化和反序列化[CP]. https://msdn.microsoft.com/zh-cn/library/bb412179(v=vs.110).aspx,2017-5-16.

[8] Kerry Jiang. SuperSocket 可扩展的Socket服务器框架[CP]. http://www.supersocket.net/,2017-5-16.

[9] 张少军,谭志.计算机网络与通信技术[M].北京:清华大学出版社,2017:109-120.

[10] 甘群文. C#多线程同步与异步的实现[D].广西:广西中医学院图书馆信息技术部,2009.

[11] 阮一峰.RSA加密算法原理[CP], http://www.ruanyifeng.com/blog/2013/07/rsa\_algorithm\_part\_two. Html,2017-5-17.

[12] 维基百科, RSA加密算法[CP], https://en.wikipedia.org/wiki/RSA,2017-5-17.

[13] 魏昭.计算机网络防御策略求精关键技术研究[D].北京:北京航空航天大学,2014.

[14] 周敬利,王晓锋,余胜生,夏洪涛. 一种新的反SQL注入策略的研究与实现[D]. 武汉:华中科技大学计算机科学与技术学院,2006.

[15] Charles Petzold.Programing microsoft windows with C#[M].上海:世界图书出版社公司,2001.

[16] 陈伟琳.协议安全测试理论和方法的研究[D].北京:中国科学技术大学,2016.

# 攻读学士学位期间发表的论文和取得的科研成果

致　　谢

本文是在我的导师史长亭老师的指导下完成的。在选题时，导师得知我对网络通信方向感兴趣，便给我建议了强调安全的“安全聊天工具的设计与实现”这个题目。当我面对私钥的传递方式不知所措时，老师给我提供了“实体token，线下传递”的设计思路。特别是最后论文的修改阶段，老师更是牺牲自己的休息时间来帮我们检查论文，及时的提出各种修改意见。老师的每一次帮助都让我感觉醍醐灌顶，一下找到了继续下去的方向。在此，我真诚的对我的老师表示感谢。

感谢哈尔滨工程大学对我大学期间的培养，这里丰富的学习资源和舒适的学习环境让我全身心的投入到学习中。在这四年中，我完成了从学校到社会的过度，掌握了学习新知识的能力，也找到了合适自己的工作。

感谢指导我学习Csharp和SuperSocket的赵晴宇老师。在实验室期间，是赵老师手把手的教导我我学习Csharp的。正是有了赵老师耐心的指导，我才有了在毕业设计中使用Csharp开发的基础和勇气。

感谢所有教导过我的任课老师，是他们细心的教学让我的基础知识更加扎实，让我的学习方向更加明确，他们的专注和严谨是我学习的楷模

感谢我身边的同学，他们让我知道协作的重要和意义。

感谢我的家人，对于我作出的每一个决定都是默默的支持和信任。现如今我即将走向社会，也不会让他们失望，我会一直努力，作一个对社会有用的人。

最后，对评审论文的各位老师表示衷心的感谢！