

《物联网安全》

设计文档

组 长： 魏来 班号： 193182

组 员： 郭鸿绅、 段依琳、 刘畅海

院（系）： 计算机学院 专业： 网络工程

指导教师： 姚 宏 职称： 教授

2021 年 5 月

目录

[1. 序言 1](#_Toc28581)

[2. 需求分析 1](#_Toc9200)

[2.1. 任务概述 1](#_Toc29110)

[2.2. 数据流图与数据字典 1](#_Toc22046)

[2.3. 状态机设计 1](#_Toc22188)

[2.4. UI布局设计 1](#_Toc18147)

[2.5. 数据库需求 1](#_Toc28427)

[3. 系统概要设计 2](#_Toc24795)

[3.1. 系统概述 2](#_Toc3717)

[3.1.1功能需求规定： 2](#_Toc30315)

[3.1.2运行环境： 2](#_Toc15735)

[3.2. 系统结构 2](#_Toc14278)

[3.3. 功能设计 2](#_Toc14194)

[3.4. 模块设计 3](#_Toc5588)

[4. 数据及状态机设计 3](#_Toc9963)

[4.1. 时序图 3](#_Toc24993)

[4.2. 数据包设计 3](#_Toc20354)

[5. 详细设计 3](#_Toc13313)

# 序言

## 1.1. 程序目的

在学习了对称加密—DES，和非对称加密—RSA之后，目前，课程设计需要将上述两种工具，以及Kerboros的认证体系结合，并应用于自定义的网络应用中。

在近期的讨论中，我们小组认为本次课程设计的重点并不在于Kerboros认证过程，而是实现一套逻辑严密，结构完整，内容丰富的网络应用，并在应用的使用过程中体现出Kerboros认证过程以及两套加解密内容；经过小组讨论并结合了现有水平能力，时间限制后，我们小组从简单的网络游戏，模拟美团点餐系统，IM（即时通讯）中敲定了本次课程设计的大致方向，即设计一套能够满足一定量并发需求的C/S模式的通讯应用，通过端到端的通讯过程，体现Kerboros认证流程与RSA加密过程，在通讯内容中体现DES加密过程。

本次应用设计中，我们将尽可能将程序模块拆开掰碎，使得模块分工细致完整，同时降低函数间，模块间的耦合度，提高程序的可拓展性；同时在实现基础通讯功能外，我还构想了邀约游戏等功能，可以理解为一套新的程序，作为一个黑盒子添加到通讯程序的拓展模块，使得程序内容更加丰富。

魏来

2021年4月28日

Ex：姓名：谈谈Kerboros、des、rsa与课程设计的关系，简述一下自己对于系统设计的想法

## 1.2. 定义

|  |  |
| --- | --- |
| **专业术语** | **定义** |
| **Kerberos** | 计算机认证协议 |
| **数据库** | 用于存放数据，租借的阿里云MySQL数据库  rm-uf6t4cbyfz681x569.mysql.rds.aliyuncs.com 端口：3306 |
| **终端** | 4台设备模拟启动6个终端，即6个设备，分为KDC和User两种类别 |
| **KDC** | 密钥分配中心，由两个终端扮演，在本次程序中分为AS终端和TGS终端 |
| **AS** | 身份验证服务，为client生成TGT的服务 |
| **TGS** | 票务发放服务，为client生成某个服务的ticket |
| **TGT** | 用于获取ticket的票据 |
| **ticket** | 用于发送信息的凭证 |
| **User** | 实际运行应用程序的设备，又分为Client，Server |
| **Server** | 通讯服务的服务器设备 |
| **Client** | 需要通讯的用户的设备 |
| **K（）** | 密钥，用于加解密工具 |
| **聊天用户** | 使用本程序的用户 |
| **Session key** | 发送应用信息时，DES加密时用到的秘钥 |

表 1 名词定义

# 需求分析

## 任务概述

本程序为基于 Kerboros 认证（DES加密）和 RSA加密的分布式通讯工具，需要实现下述功能：

工具：

1. 加密工具：使用DES与RSA两种加密方式，根据报文的不同需求，分别使用不同的加密方式。
2. RSA加密中的证书：约定好证书格式后，每个设备启动时，都会生成自己的证书，同时我们认为这个证书在系统内，独一无二，绝对真实，绝对安全，因此，先通过明文通讯，使得所有User设备与KDC设备间得到对方的公钥，即证书互信。同时可以认为系统内的Client与Server间都有对方的公钥，传输后续DES加密用到的session key。

Kerberos认证：

1. Kerberos认证体系：当所有设备启动后，其中两台设备扮演TGS和AS的角色，一台设备扮演通讯工具中的Server，其他设备扮演Client；所有Client和Server根据自己在AS中的账号登录验证身份，AS和TGS为每一个Client与Server间提供认证服务，Client与Client间没有必要提供认证服务。
2. 在Kerberos认证之前：由于Kerberos本身无RSA加解密需求，但为了将该功能引入Kerberos中，我们将最开始认证中出现的作为明文，根据最初已经获得的证书信息，使用RSA加密，通过通信功能传输。
3. 通过上述顺序为4）---> 3）--->2）的逻辑，实现了Kerberos认证功能后，认为除了出现新的User设备，整个系统内无需再使用Kerberos认证，AS和TGS设备监听新设备，不执行后续逻辑功能。

通讯工具：

1. 加好友：Client A向Server发送添加Client B为好友的请求，Server将此请求转发给Client B，Client B再将回复信息发送给Server，Server继续转发。
2. 加群聊：邀请加群，一个Client向多个Client发送邀请，方式同6）；申请入群，一个Client向拥有群的Client发送申请，方式同6）。
3. 删除好友、退出群聊：Client A向Server发送删除好友Client B的信息，Server更改二者数据库信息。
4. 聊天：Client A与Client B或多个Client的即时通讯，通过Server转发。
5. 搜索功能：提供Search界面，某个Client可以输入某些关键词，Server会根据内容在系统数据库中查找并将一定信息返回给Client。
6. 登录界面：每个用户输入账号密码，登录聊天程序
7. 注册，修改密码+拓展（忘记密码）：通过网页修改，Server修改Server数据库。
8. 聊天记录存储在本地log文件中。

## 模块设计

因此程序将从整体分为四大模块，如下所示：

1. 加解密模块：分别实现DES、RSA加解密功能，为其他模块调用提供接口
2. Kerberos认证模块：为User设备提供认证服务，使得User间都有各自间通信的session key。
3. 网络通讯模块：提供设备间通讯的框架
4. 应用模块：实现通讯协议，将User分为Client和Server设备，实现Client间的即时通讯功能。

以六台设备为例，当六台设备分别作为KDC和User启动时，KDC将会作为AS和TGS为User提供Kerberos的认证服务，认证完成后，作为KDC的两台设备不参与应用模块；认证后，每个独立的Client与Server间都存在一个Session key，为应用模块服务，应用模块实现即时通讯的逻辑功能。

同时通讯模块与加密模块作为工具模块，为Kerberos认证和应用提供接口，实现数据的加解密，以及用户间数据的发送。

模块功能图如下所示：

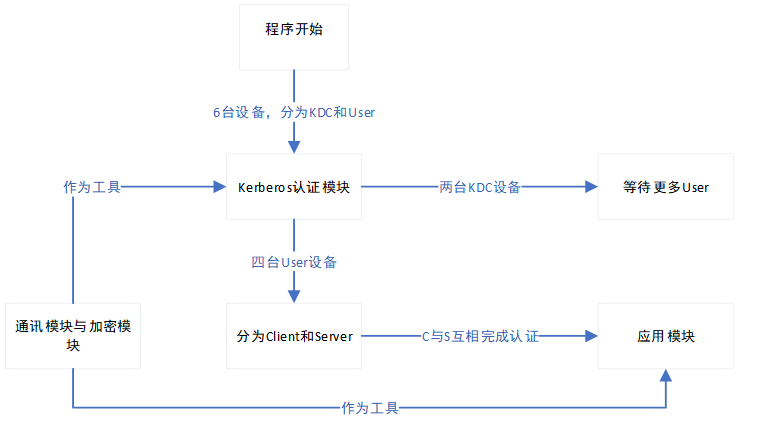


图 1 模块功能图

本次程序验收功能框架如下表：

Ex：表2.

## 数据流图

### 顶层数据流图



图 2 顶层数据流图

### 一层数据流图



图 3 一层数据流图

### P1二层数据流图



图 4 P1二层数据流图

### P2二层数据流图



图 5 P2二层数据流图

### P3二层数据流图



图 6 P3二层数据流图

## 状态机设计

### AS状态机



图 7 AS状态机

### TGS状态机



图 8 TGS状态机

### Client状态机



图 9 Client 状态机

### Server状态机

## UI布局设计

Ex：商榷，登录界面可以白嫖

## 数据库需求

### 数据字典

### ER图

Ex：er图，存放数据

# 系统概要设计

## 系统概述

### 3.1.1功能需求规定：

Ex：学生信息管理系统完成对学生信息的管理，包括添加用户账号，修改用户信息，删除用户信息

### 3.1.2运行环境：

运行平台：

数据库：

Web：

开发语言：

## 系统结构



## 功能设计

Ex：画图中

## 详细模块设计

Ex：画图中

# 数据

## 时序图

Ex：Visio画图，类似于握手挥手协议模块

## 数据包设计

Ex：xxx，yyyy，zzzz，tttt，

xxx为首部，编码xxx，表示xxx

Yyyy为数据内容

Zzzz为时间戳

Tttt为数字签名

# 详细设计

## 错误码

## 模块详细设计

## 函数设计

## 函数流程图

## 甘特图

Ex：具体函数代码，传入传出，有待商榷