# WChat技术介绍

## 服务器技术

主要框架：

Springboot 版本2.2.0.RELEASE

Websocket 即时通讯支持

mybatis 持久化支持

Tomcat（springboot内置）容器支持

使用软件：

Idea 后台开发工具

Maven 依赖管理工具

Navicat 数据库查看工具

Mysql 数据库持久化

其他依赖技术：

Junit 单元测试支持

Fastjson json支持

Lombok 代码生成插件

Druid 数据库连接池管理

Pagehelper 分页插件

Bouncycastle 加解密支持

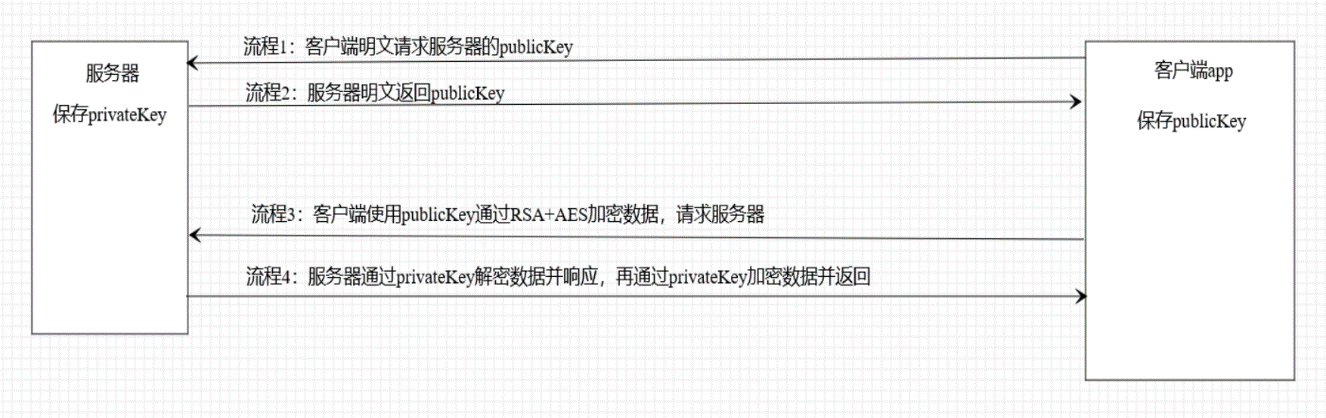
## Android端技术

## 安全方案

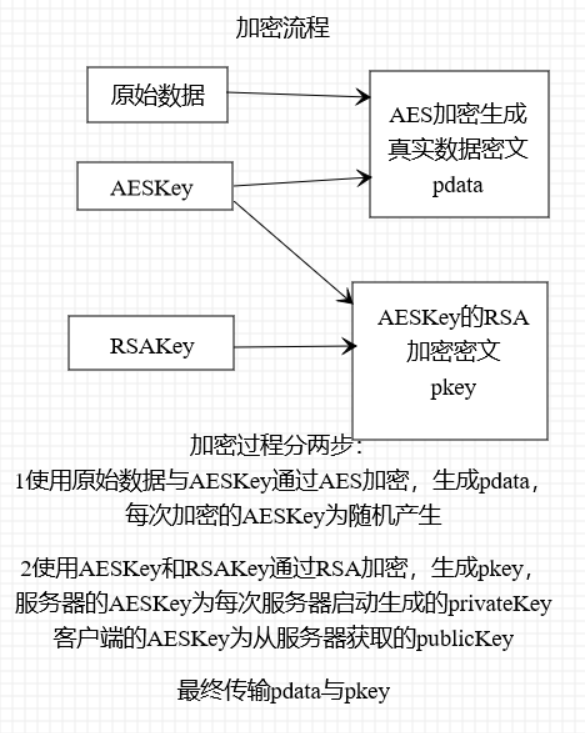
1. 信息传输安全

采用AES+RSA双重加密，保证数据安全

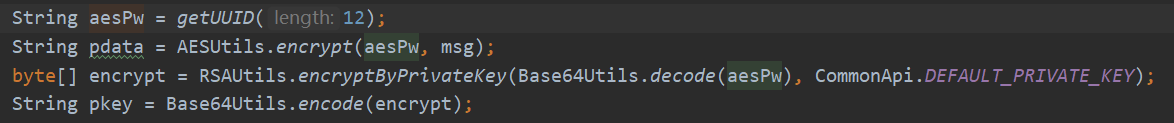
加密传输流程如下图：



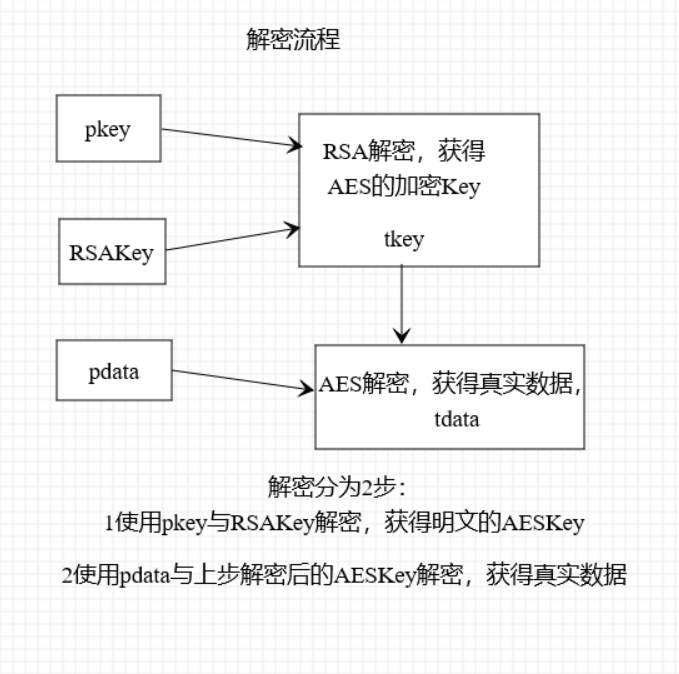
加密流程如下图：



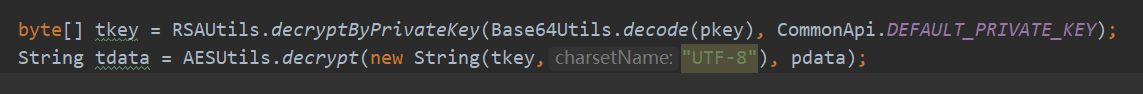
加密代码：



解密流程如下图：



解密代码：



1. 服务器端安全

Xss防御

com.wchat.utils.XssUtils工具类，在每次请求时，过滤危险请求内容，替换危险字符，实现Xss攻击防御。

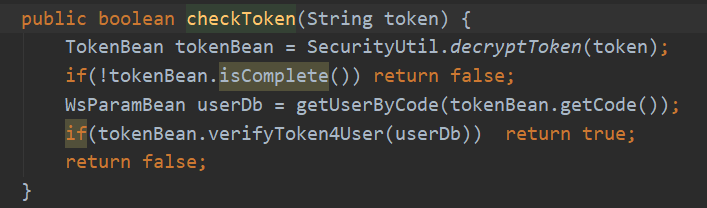
Xss防御代码：



Csrf防御

敏感请求都会有token验证，token无效则不能执行操作，实现csrf攻击防御

Csrf防御代码：



1. 秘钥安全

AESKey每次加密随机生成，增加安全性

PrivateKey 服务器每次启动重新生成，增加安全性

PublicKey 客户端每次去服务器获取

## 部署说明

1. 安装JKD8
2. 安装mysql，可调用远程服务：116.62.12.140
3. 复制jar包到本地
4. 在jre安装目录中添加jar包
5. 在jre安装目录中找到java.security，添加行security.provider.11=org.bouncycastle.jce.provider.BouncyCastleProvider
6. 双击启动快捷方式(startup.bat)，系统启动，部署完成。

## 操作说明

1. 服务器启动
2. 安装客户端app
3. 打开app
4. 设置服务器地址，如设置失败，则服务器未成功启动
5. 注册or登陆
6. 点击用户名称，进入聊天页面
7. 输入信息，发送信息