2022全国大学生信息安全竞赛创新能力赛

预赛可信计算赛题1：基于挑战码的双向认证

## 一 题目描述：

本题考察学生对用户身份认证协议的理解。

现有用户终端term与服务器server，用户alice拟通过term登录server，alice与server共享密钥key。为防止重放攻击，term与server间拟采取基于挑战码的双向认证协议，其过程如下所述：

1. term生成随机数rA,并向server端发送。
2. server端生成随机数rB，计算MB=SM3(key, rA||rB),并向term发送rB 与MB。
3. term计算MB’= SM3(key, rA||rB),并与MB比较，若一致则确认服务器端正确。
4. term计算MA=SM3(key,rB),并将MA发送给Server
5. Server计算MA’=SM3(key,rB),并与MA比较,若一致则确认客户端登录正确。

客户端登录功能由user\_client模块执行，服务器端登录功能由user\_server模块执行。

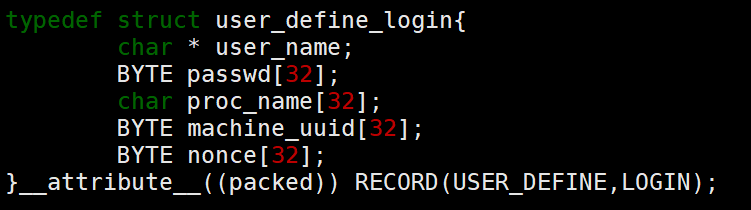
user\_server模块已完成，user\_client模块尚未完成，请你完成user\_client模块，并通过测试程序的验证。

## 二 题目环境：

本题目为“兵棋”模式新型可信计算赛题，示例在docker环境下运行，基于可信软件基原型Cube-1.3搭建，通过分布式消息驱动机制模拟应用流程与攻防行为。

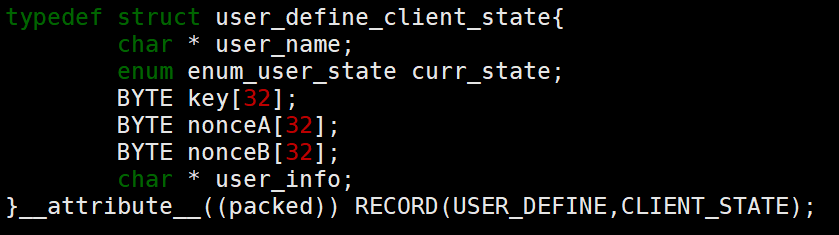
选手以player用户身份登入系统。题目提供测试环境与评分环境。两环境中均各有一服务实例cube-challenge/instance/server、一个用户实例cube-challenge/instance/user,和一个非法服务器实例cube-challenge/instance/hacker\_server，分别模拟合法服务器端、用户终端和非法服务器端。

系统中用户登录数据的格式定义在include/user\_define.h中，如下所示：

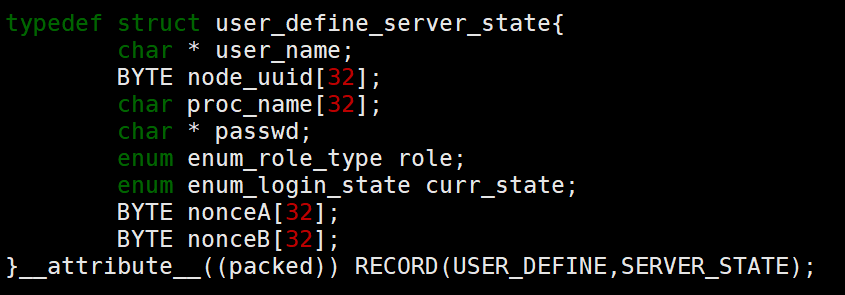


双方前三次交互均使用这一结构。这里passwd用来存放认证相关数据（sm3计算结果），nonce则用来存放双方交换的随机数。

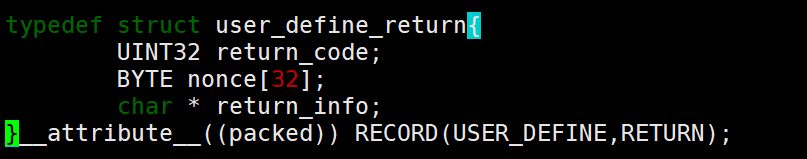
用户终端建立下面结构作为认证过程中的上下文，储存处理过程中的信息。



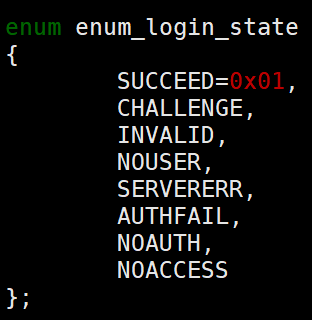
服务器端则为所有登录用户建立内存数据库，存放如下格式的信息，在登录认证过程使用。



登录过程中失败或最后通过整个登录验证过程时，将返回下面结构：



这里return\_code返回登录结果，有下面的取值选项:



用户登录时，部分用户将正常连接server端，由user的Login\_user模块(源码在src/login\_user目录)和server端的login\_server模块（源码在src/login\_server目录）完成登录过程，但部分用户会与hacker\_server端连接，hacker\_server端将冒充正常服务器端，但其没有用户的密钥。

请修改login\_user模块的proc\_login\_response函数，完成对服务器端的验证，如服务器未通过验证则以（USER\_DEFINE,RETURN）格式输出错误信息（可参考login\_server模块的错误信息输出方式）,如服务器通过验证，则执行认证过程的第4步，用计算结果填充待发送的（USER\_DEFINE,LOGIN）数据格式，以完成合法用户的认证过程。完成代码修改后，需编译Login\_user模块（可直接在目录下执行make命令）,而后在cube-challenge目录下用login-challenge.sh脚本测试登录过程。

测试通过后，用户可执行sh player.sh，即可通知root端启动评分环境中各种实例，测试用户访问控制机制的正确性，并根据测试结果，决定不产生输出、产生1个flag或产生2个flag。

## 三 解题要求

选手修改player目录下cube\_challenge/src/login\_user模块，参考注释添加正确的服务器验证与验证数据生成机制，而后编译，编译时需配置CUBE架构相关环境变量，其中Cube架构的基本环境变量已配置，选手只需直接执行make命令即可编译。

系统本地测试通过后，可执行sh player.sh启动评分环境，评分环境会提示进行测试的内容，完成测试后，根据测试结果确定用户获取flag情况，并输出flag。

## 四 题目提示

可参考其它模块类似功能部分的代码。

。