

网络安全实验报告

题 目 基于口令的认证过程实现

专 业 计算机科学与技术

学 号 7203610316

学 生 符兴

指 导 教 师 王彦

# 一、实验目的

掌握随机函数的使用，掌握散列函数，加解密函数的使用。包的格式与发包的顺序，可以等同于协议的三要素。掌握程序与数据库的链接。

1. **实验内容**

1. 客户端输入用户名，口令，随机产生认证码，使用散列函数计算用户名与口令的散列值1，使用散列值1与认证码计算散列值2，将用户名，散列值2，认证码明文传送到服务器端。

2. 服务器端以数据库（如access）保存用户名和散列值1的对应关系。收到客户端信息后，以同样的方法计算散列值2’。 如散列值2’=散列值2，则认证成功，成功后用散列值1加密认证码发送给客户端。客户端解密后写到指定文件。用户可以修改自己的密码。。

# 三、实验过程

**基于口令的认证过程实现**

**实验基本信息：**

实验环境：Windows11 x64，Mysql8.0

编程语言：Python

## 1. 需求分析

需要编写服务端和客户端相应的程序，并且按照一定的协议实现消息的加密发送，其中比较重要的功能函数有：

1. 随机认证码的生成
2. 散列函数
3. DES加解密算法

## 2. 程序结构

(1) 客户端程序的大致结构为：

① 通过TCP协议连接服务器。

② 正确连接服务器后，用户键入用户名、口令，等待认证。

③ 生成随机认证码a，计算用户名和口令的散列值b；然后计算随机认证码a和散列值b的散列值c。

|  |
| --- |
|  |
| 图1 准备数据阶段代码截图 |

④ 将用户名，散列值c以及随机认证码明文发送到服务器端，等待服务器的认证。

⑤ 若认证成功，可以通过随机认证码对服务端发送来的消息进行解密，并写入相应的文件中。在这里，消息的加密算法为DES，加密的密钥是散列值b。

|  |
| --- |
| 文本  描述已自动生成 |
| 图2 等待服务器发送认证结果 |

⑥ 用户可以向服务器发起修改密码的请求。

⑦ 获取用户新的密码，并重复2的过程；但是在发送时候需要将散列值b发送给服务端，因为服务端需要保存该散列值用于后续的认证。

|  |
| --- |
|  |
| 图3 用户修改密码过程 |

(2) 服务端程序的大致结构为：

① 监听连接请求

|  |
| --- |
|  |
| 图4 服务端认证过程 |

② 在收到一个连接认证请求时，服务端需要对其进行认证。首先通过用户名在数据库查找用户对应的散列值b，然后将散列值b和接收到的随机认证码生成新的散列值c’，将新散列值c‘和接收的散列值c进行比对；如果二者相同则认证成功；如果二者不同，则认证失败；

③ 如果当前用户认证成功，则服务端会使用用户的散列值b对一个消息进行加密并将其发送给客户端；

④ 如果当前用户发送修改密码请求，服务端会接受来自客户端的用户名，散列值b和随机认证码；然后将数据库中该用户对应的散列值更新为新的散列值b；完成更新后向客户端发送响应。

|  |
| --- |
|  |
| 图5 服务端相应客户端修改密码请求 |

(3) DES加解密算法的大致结构为：由于算法限制，这里的密钥取得是所输入散列值的前8位；

|  |
| --- |
|  |
| 图6 DES加密 |
|  |
| 图7 DES解密 |

# 四、实验结果

(1) MySql数据库保存的用户信息：

|  |
| --- |
|  |
| 图8 数据库保存的信息 |

(2) 程序运行截图：

|  |
| --- |
|  |
| 图9 客户端流程截图 |
|  |
| 图10 服务端流程截图 |

(3) 客户端将消息解密并写入文件中（这里使用了自定义的消息）：

|  |
| --- |
|  |
| 图11 客户端解密消息写入文件 |

# 五、心得体会

(1) 进一步了解对消息加密发送的过程，并掌握了散列函数，DES加密算法。

(2) 更深入了解了网络中两台主机之间发送数据的具体过程，并通过自定义的协议实现对消息的加密传送，并且在接收端可以正确解密并写入对应的文件中；