第三章 课后作业

1、我们知道，在 UNIX 系统的口令方案中引入盐值大大地增加了口令猜解的难度（难度是原来的 4096 倍）。但是，盐值以明文的形式和经过加密的口令一起存放在口令文件中，攻击者无需猜测就可以得到盐值以及加密的口令。那么，为什么可以断言使用盐值能够提供口令的安全性？

•盐值可以防止复制的口令在口令文件中可见。即使是两个不同的用户选择了相同的口令，这些口令也会被分配到不同的“盐值”。因此，这两个用户所拥有的散列口令是不同的

• 盐值显著地增加了离线口令字典攻击的难度。对于一个 n 位长度的“盐值”，可能产生的口令数量将会增加2^b倍，这将大大增加通过字典攻击来猜测口令的难度。

• 盐值使得攻击者几乎不可能发现一个用户是否存在两个或更多系统中使用了相同的口令。

2、目前网络上都有哪些措施用于避免口令猜测？如果是你设计的系统，你会怎么设计？

- 严格限定从一个给定的终端进行非法认证的次数;
- 防止用户使用太短的口令;
- 使用机器产生的口令

设计：

- 密码长度要求在 10-18 位。
- 密码要是大写字母、小写字母、数字、符号中的三种的组合
- 密码中不能出现自己的生日等常见信息
- 当输入密码认证失败 5 次后，将 ID 进行冻结

3、如果行李箱的密码忘了，可以用什么办法解决？三位密码，有多少种可能？

可以采用暴力破解的方式进行破解，对于一个三位数的密码，只有$10^3 = 1000$种可能的情况，可以在一个较短的时间内成功解密

4、目前银行普遍使用的磁条卡和芯片卡的区别有哪些？请问磁条卡和芯片卡哪种更安全？为什么？

区别：

一、介质不同

芯片银行卡是以芯片作为介质的银行卡，卡的正面有一个芯片，支持闪付功能。而磁条卡是利用磁性载体记录英文与数字信息，用来标识身份或其它用途的卡片。

二、安全系数不同

芯片卡的容量大（储存量是磁条卡的 160 倍），可存储密匙、数字证书、指纹等信息，卡上有读写保护好数据加密保护，并且在使用保护上采取个人密码、卡与读写器双向认证，防止卡片数据被复制，具有更高的安全性。磁条卡在通过写磁设备后会被不法分子利用进行伪卡的盗刷，安全系数较低。

三、工作原理不同

芯片卡比磁条卡多了个芯片，在付款时除了要刷磁条外，还要验证芯片。

安全性：

芯片卡比磁条卡更加安全，两种卡记录身份信息的方式也不一样，磁条卡是用磁信号记录信息，而芯片卡则是电子芯片记录信息。因为磁条卡容易被复制，所以安全性较低，芯片卡很难复制，反之安全性更高。