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？

答：

对于用盐值进行加密的口令来说，攻击者虽然知道盐值的明文和加密后的口令，但是无法通过单向散列函数求得原来的口令明文，相比于不使用盐值的系统来说，攻击者除了必须要提供一个猜测的口令进行散列运算外，还要考虑字典文件中的每一个‘盐值’，这就使得需要检查的猜测次数大大增大。

盐值保证了，不用的用户得到的盐值是不一样的，最大程度上保证了安全性，其次，它还可以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的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？

答：

口令文件访问控制，拒绝对手访问口令文件，如果文件的散列口令部分只能被特权用户访问，那么对手就不能读取口令文件。

计算机生成口令，避免用户设置的口令过于简单。

后验口令检查，系统周期性地运行自己的口令程序来找到容易被猜测到的口令，系统将会取消这种容易被破解的口令。

先验口令检查，在用户设置口令过程中，进行检查口令的安全性。

如果是我设计的系统，首先我会在用户密码复杂度上进行高级的设置，不允许设置安全性较差的密码，其次我会设置密码的长度够长，只能允许特定的权限才能访问口令文件，最后增大盐值的长度，增加攻击低手破译密码的难度。

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？

答：

因为是三位的密码，所以最终所有可能为 1000 种可能，因为每一位都有 10 种可能，如果行李箱密码忘记的话，第一种方法是可以暴力破解法，试一千次。第二种办法是通过听行李箱内部的声音，如果某一个密码卡到了正确的位置，会发出不一样的声音，以此找到正确的密码。

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？

答：

磁条卡是为刷入卡片上的黑色磁条进行读写信息，而芯片卡是为插入卡片读写信息，芯片卡的安全性要高于磁条卡，因为芯片卡的抗攻击能力强，很难去复制，不会出现消磁的情况，磁条卡的安全性相对较低，容易被窃取信息，从而盗刷。芯片卡会采取个人密码、卡与读写器双向认证。因此芯片卡被攻击的难度更高。