第3讲测试点

姓名：袁昊男 学号：2018091618008

**检测点3-1**

编制一个口令强度检测程序（语言不限）要求如下：

* 口令必须包含大写字母，小写字母，数字，特殊字符四种中的三种，长度要求8到30位。
* 提供源码和运行截图。

1. 源代码

|  |
| --- |
| 1. **import** re 3. **def** password\_test(password): 4. key = True 5. **if** len(password)<8 **or** len(password)>30: 6. key = False 7. NumRegex\_0 = re.compile(r'[A-Z]').search(password)    # 大写字母 8. NumRegex\_1 = re.compile(r'[a-z]').search(password)    # 小写字母 9. NumRegex\_2 = re.compile(r'[0-9]+').search(password)   # 数字 10. NumRegex\_3 = re.compile(r'[~!@#$%^&\*()=+[\\]{}''\";:/?.,><`|！·￥…—（）\\-、；：。，》《]').search(password)   # 特殊字符 12. count = 0 13. **if** (NumRegex\_0 != None): 14. count = count + 1 15. **if** (NumRegex\_1 != None): 16. count = count + 1 17. **if** (NumRegex\_2 != None): 18. count = count + 1 19. **if** (NumRegex\_3 != None): 20. count = count + 1 22. **if** (count < 3): 23. key = False 24. **if** key: 25. **print**('口令满足要求') 26. **else**: 27. **print**('口令不满足要求') 29. **if** \_\_name\_\_ == '\_\_main\_\_': 30. **while**(True): 31. password = input('请输入口令: ') 32. password\_test(password) |

1. 运行截图



**检测点3-2**

1、针对基于密码的身份认证，主要存在重放攻击和中间人攻击两种安全风险，试分析基于对称密码的Needham-Schroeder协议流程，判断该协议是否存在安全风险？如果存在，请给出攻击过程和改进方案。

**答：**基于对称密码的Needham-Schroeder协议主要存在重放攻击风险。原始Needham-Schroeder协议步骤如下：

1. *A* → *S*: *A*, *B*, *NA*
2. *S* → *A*: {*NA*, *B*, *KAB*, {*KAB*, *A*}*KBS*}*KAS*
3. *A* → *B*: {*KAB*, *A*}*KBS*
4. *B* → *A*: {*NB*}*KAB*
5. *A* → *B*: {*NB*-1} *KAB*

攻击过程是：在第(3)步，若攻击者能获取*A*、*B*以前的一次会话，则攻击者拥有以前的{*KAB*', *A*}*KBS*，攻击者在第(3)步可冒充*A*将{*KAB*', *A*}*KBS*发送给*B*，*B*接受后以旧会话密钥*KAB*'与攻击者建立通信，重放攻击成功。

改进方案：在第(2)步和第(3)步中加入时间戳*T*，改进后的协议步骤如下：

1. *A* → *S*: *A*, *B*, *NA*
2. *S* → *A*: {*NA*, *B*, *KAB*, {*KAB*, *A*, *T*}*KBS*}*KAS*
3. *A* → *B*: {*KAB*, *A*, *T*}*KBS*
4. *B* → *A*: {*NB*}*KAB*
5. *A* → *B*: {*NB*-1} *KAB*

这样，*B*在接收{*KAB*, *A*, *T*}*KBS*后先验证*T*，当*T*与当前时间的误差在一定范围内时，*B*接收会话密钥*KAB*并与*A*相互建立通信，可在一定程度上避免重放攻击。但还存在等待重放攻击风险：如果发送方的时钟超前于接收方的时钟，攻击者就可截获发送方发出的消息，等待消息中时戳接近于接收方的时钟时，再重发这个消息。这种重放可造成重复接收等问题。

2、使用公钥密码的Needham-Schroeder协议流程如下：

1. *A* → *B*: *EB* (*NA, A*)
2. *B* → *A*: *EA*(*NA, NB*)
3. *A* → *B*: *EB*(*NB*)

分析该协议中存在的安全风险，给出攻击过程和改进后的方案。

**答：**基于公钥密码的Needham-Schroeder协议主要存在中间人攻击风险。假设中间人为*I*，位于*A*、*B*之间传递消息。攻击过程如下：

1. *A* → *I*: *EI* (*NA, A*)
2. *I* → *B*: *EB* (*NA, A*)
3. *B* → *I*: *EA*(*NA, NB*)
4. *I* → *A*: *EA*(*NA, NB*)
5. *A* → *I*: *EI*(*NB*)
6. *I* → *B*: *EB*(*NB*)

攻击者在第(1)步后解密得到消息*NA*、在第(5)步后解密得到消息*NB*并向伪装*A*向*B*发送消息；*B*认为其与*A*共享秘密，实际上*B*与*I*共享秘密，*I*假冒*A*成功，中间人攻击成功。

改进方案：在原始协议流程第(2)步中增加发送者身份，可有效避免中间人攻击。改进后的协议步骤如下：

1. *A* → *B*: *EB* (*NA, A*)
2. *B* → *A*: *EA*(*NA, NB, B*)
3. *A* → *B*: *EB*(*NB*)