计算机密码学理论与应用

关于身份认证类协议的习题

习题1(参阅Stallings 习题15.7)：一种双向身份认证协议及其攻击实例

以下是双向身份认证协议，$Sig_A(x)$表示x及用A的私钥对x生成的数字签名，N_A是A生成的随机数，t_A是A的本地时间，ID_A是A的身份标识，等。

1. A←B: initiation, ID_B
2. A→B: $Sig_A(t_A, N_A, ID_B)$
3. A←B: $Sig_B(t_B, N_B, ID_A, N_A)$
4. A→B: $Sig_A(N_B)$

(1) 准确、完整地表述该协议在A、B进程中的完整动作。

【从编程的角度，对进程A、B的处理动作分别阐述】

(2) 如果协议不使用动态时钟，是否安全（抵抗身份欺诈）？

分析下面的例子。

习题1(Stallings 参考习题15.7)：续

（2）不使用时钟的情况：C是攻击者、A和B是诚实的参与方

1. A←B: initiation, ID_B
2. A→B: $Sig_A(0, N_A, ID_B)$
3. A←B: $Sig_B(0, N_B, ID_A, N_A)$
4. A→B: $Sig_A(N_B)$

A、B之间的某轮协议会话

5. A←B: initiation, ID_B
6. C阻塞消息5
7. C→B: $Sig_A(0, N_A, ID_B)$
8. C/A←B: $Sig_B(0, N^*_B, ID_A, N_A)$
9. C→B: $Sig_A(N^*_B)$

C拟向B冒充自己是A

10. A←C: initiation, ID_C
11. A→C: $Sig_A(0, N^*_A, ID_C)$
12. A←C: $Sig_C(0, N^*_B, ID_A, N^*_A)$
13. A→C: $\mathbf{Sig_A(N^*_B)}$

14(9). C→B: $\mathbf{Sig_A(N^*_B)}$

* 在第12.步之后，A达到什么判定状态？在第14步后，B达到什么判定状态？
* A、B两者的判定状态是否与双向身份认证目的一致？
* **(3)** 如果各方使用本地的动态时钟，上述欺诈是否还起作用？
* 更准确地说：协议进程应如何处理时钟信信息，能使上述攻击失效？

习题1(Stallings 参考习题15.7)：续

(4) 看下面不使用时钟的协议设计：

1. A←B: initiation, ID_B
2. A→B: $Sig_A(N_A, ID_B)$
3. A←B: $Sig_B(N_B, ID_A, N_A)$
4. A→B: $Sig_A(N_B, N_A)$

准确、完整地表述该协议在A、B进程中的完整动作。

(5) 以上协议是否能抵抗前述攻击/身份欺诈？试给出分析说明。

根据你的分析，检查你在(4)中的陈述是否准确、完整！

【答案参阅最后一页PPT；请先独立思考】

习题2(参阅Stallings 习题15.9)

* 分析以下单向认证协议，R表示随机数，E是某种安全的公钥加密方案。
* (1) 准确、完整地表述该协议在A、B进程中的完整动作。
* 【从编程的角度，对进程A、B的处理动作分别阐述】
* (2) 该协议并不安全，试给出一种欺诈攻击途径。
* (3) 试改进该协议，并准确、完整表述协议在A、B进程中的完整动作。

* 1. A←B: initiation, ID_B
* 2. A→B: ID_A
* 3. A←B: $E_A(R_B)$
* 4. A→B: R_B

* 【参考答案见下页；请先独立思考】

习题2(参阅Stallings 习题15.9)：一种欺诈途径

C拟向B冒充自己是A

* 5. A←B: initiation, ID_B
* 6. C阻塞上述消息
* 7. C→B: ID_A
* 8. C/A←B: $E_A(R_2)$
* 9. C→B: R_2

* 10. A←C: initiation, ID_C
* 11. A→C: ID_A
* 12. A←C: $E_A(R_2)$
* 13. A→B: R_2

* 14(9). C→B: R_2

习题2(参阅Stallings 习题15.9)：一种改进

* 改进的协议
* 1. A←B: initiation, ID_B
* 2. A→B: N_A, ID_A
* 3. A←B: $E_A(N_A||R_B)$
* 4. A→B: R_B

C拟向B冒充自己是A

* 5. A←B: initiation, ID_B
* 6. C阻塞上述消息
* 7. C→B: N, ID_A
* 8. C/A←B: $\mathbf{E_A(N||R_2)}$
* 9. C→B: R_2

* 10. A←C: initiation, ID_C
* 11. A→C: N^*, ID_A
* 12. A←C: $\mathbf{E_A(N||R_2)}$
* 13. A→B: $\mathbf{R_2}$

C这样做还可行吗？A预期解密后应该看到什么样的明文？理解这一点后，相应的处理应该成为进程A动作的一部分。

* 14(9). C→B: $\mathbf{R_2}$

【注】(x,y,z)和x||y||z等均表示数据项的顺序连结。下同。

习题1(Stallings 参考习题15.7) 参考答案

（4）新版协议在面向原攻击时的情况：C是攻击者、A和B是诚实的参与方

A、B之间的某轮协议会话

1. A←B: initiation, ID_B
2. A→B: $Sig_A(N_A, ID_B)$
3. A←B: $Sig_B(N_B, ID_A, N_A)$
4. A→B: $Sig_A(N_B, N_A)$

5. A←B: initiation, ID_B
6. C阻塞消息5
7. C→B: $Sig_A(0, N_A, ID_B)$
8. C←B: $Sig_B(0, N^*_B, ID_A, N_A)$
9. C→B: $Sig_A(N^*_B, N_A)$

A拟向B冒充自己是A

10. A←C: initiation, ID_C
11. A→C: $Sig_A(0, N^*_A, ID_C)$
12. A←C: $Sig_C(0, N^*_B, ID_A, N^*_A)$
13. A→C: $\mathbf{Sig_A(N^*_B, N^*_A)}$

14(9). C→B: 这里C还能利用$\mathbf{Sig_A(N^*_B, N^*_A)}$来欺骗B让其相信对话的是A吗?

*

一些存在缺陷的协议实例

* 参阅：
*
* Bruce Schnerier 应用密码学，机械工业出版社，2001
* 田园 网络安全教程，人民邮电出版社，2009，第九章。