doi:10.3969/j.issn.1007-855x.2010.02.016

Denning-Sacco密钥分配协议的分析与改进

缪祥华
(昆明理工大学 信息工程与自动化学院,云南 昆明 650051)

摘要: 研究了 Denning-Sacco密钥分配协议,指出了该协议存在的缺陷和漏洞,并给出了两种攻击该协议的方法,一种是重放攻击,另一种是拦截攻击.虽然一些学者对该协议进行了修改,但是仍然存在缺陷和漏洞.针对原始协议存在的缺陷和漏洞,该文在原来协议的基础上,增加了一条消息,并用串空间模型来分析了修改后的协议,说明修改后的协议能够达到协议的目标.

关键词: 协议分析;串空间; Denning-Sacco密钥分配协议
中图分类号: TP309 文献标识码: A 文章编号: 1007-855X(2010)02-0076-05

Analysis and Improvement of Denning-Sacco Key Distribution Protocol with Public Key

MIAO Xiang-hua
(Faculty of Information Engineering and Automation, Kunming University of Science and Technology, Kunming 650051, China)

Abstract Denning-Sacco key protocol with public key is researched in this paper. The bugs and leaks existing in the protocol are pointed out. Two methods to attack the protocol are then put forward, namely replaying attack and holding up attack respectively. A message is added to the protocol to improve it. Finally, strand space model is adopted to analyze the improved protocol, the result of which indicates the feasibility of the method.

Key words protocol analysis; strand space; Denning-Sacco key distribution protocol with public key

0 引 言

20多年来,安全协议的分析一直受到重视和广泛关注,专家和学者们提出了很多分析安全协议的形式化方法.纵观这些安全协议的形式化分析方法,基本上可以分为三类,即基于逻辑推理的分析方法[1]、基于模型检测的分析方法[2]和基于定理证明的分析方法[3].串空间模型[4-7]是基于定理证明的分析方法的代表,它集成了其它基于定理证明的分析方法的优点于一身.本文所用的分析方法就是串空间模型,串空间模型的基本内容见文章的第 1部分. Denning-Sacco[8]密钥分配协议提出以后,受到大家的重视,很快发现该协议存在漏洞,典型的攻击方式为重放攻击,虽然可以在消息中加上主体的名字来避免发生重放攻击,但是仍然不能抵抗拦截攻击.针对该协议存在的问题,本文修改了 Denning-Sacco密钥分配协议,在原来协议的基础上,增加了一条消息,然后利用串空间模型分析了修改后的协议,说明修改后的协议能够达成协议的目标.

1 串空间模型

本部分主要介绍串空间模型,关于串空间的详细内容请参考文献[4-7].

收稿日期: 2009-03-10.基金项目: 云南省教育厅资助项目(项目编号: 07C10075);昆明理工大学科学研究基金项目(项目编号: 2007-29).

第一作者简介: 缪祥华(1972-),男,副教授,博士.主要研究方向: 信息安全理论与技术.
E-mail: xianghuamiao@126.com

串 (strand)是协议中的主体可以执行的事件序列. 对于诚实的主体, 该事件序列是由协议定义好的, 由发送消息的事件和接收消息的事件所组成; 对于攻击者, 该事件序列由攻击者的行为来确定. 串空间 (strand space)是诚实的主体串和攻击者串所组成的集合. 束 (bundle)是串空间的一个子集, 用来表示一个完整的协议. 束是一个有限无环图, 每个结点由两部分组成, 即 < 串名, 位置 >, 其中串名指出该结点所属的串的名称, 位置指出该结点在串中的位置编号. 束中有两种边, 这两种边表示了结点间的因果依赖关系. 第一种边: $< s, i > \rightarrow < s_1, i_1 >$, 表示串 s中的第 i个结点发送消息给串 s_1 中第 i_1个结点; 第二种边: $< s, i > \Rightarrow < s, i+1 >$, 表示结点 $< s, i >$ 是结点 $< s, i+1 >$ 的直接前驱. 在串空间模型中, 协议的正确性问题可以表示为不同串之间的因果连接关系.

1. 1 术语 (term)和子术语 (subterm)

协议参与者可能交换的消息称为术语, 一个协议中所有参与者间可能交换的术语集合记为 A. 原子术语分为两种: 一种是明文术语 (比如参与者标识、随机数等); 另一种为密钥术语 (包括对称密钥、非对称密钥等). 因此术语集 A 被划分为明文术语集 T 和密钥术语集 K 两部分.

术语可递归定义如下:

(1)若 m 是明文术语或密钥术语, 则 m 是术语;

(2)若 m 是术语, k是密钥术语, 则 $\{m\}_k$ 是术语 (表示将 m 用 k加密);

(3)若 m, n均是术语, 则 (m, n)也是术语 (表示将 m 和 n进行连接).

定义 **1**　一个符号术语是一个二元组 $< \delta, a >$, 其中 δ是一个符号, 为 + 或者 -, $a \in A$, 一个符号术语写为 $+a$或 $-a$. $(\pm A)^*$ 表示符号术语的有限序列集合, $(\pm A)^*$ 的元素表示为 $(< \delta_1, a_1 >, < \delta_2, a_2 >, \cdots, < \delta_n, a_n >)$.

定义 **2**　术语 a是术语 b的子术语, 即 $a \sqsubset b$, 如果 a和 b满足以下的某一个条件:

(1)若 $b \in T$, 则要求 $b = a$;

(2)若 $b \in K$, 则要求 $b = a$;

(3)若 $b = \{g\}_k$, 则要求 $a \sqsubset g$或 $\{g\}_k = a$;

(4)若 $b = gh$, 则要求 $a \sqsubset g$或 $a \sqsubset h$.

1. 2 strand, strand space和 bundle

串 (strand)是协议中的主体可以执行的事件序列. 对于诚实的主体, 该事件序列是由协议定义好的, 由发送消息的事件和接收消息的事件所组成; 对于攻击者, 该事件序列由攻击者的行为来确定. 串空间 (strand space)是诚实的主体串和攻击者串所组成的集合.

定义 **3**　一个 strand space是一个集合 S, 以及映射 $tr: S \rightarrow (\pm A)^*$, 满足下面的条件:

(1)结点是一个有序对 $< s, i >$, $s \in \sum$, i满足 $1 \leqslant i \leqslant length(tr(s))$. 结点 $n = < s, i >$ 属于 *strand* s, 表示为 $n \in s$ 结点的集合记为 N.

(2)如果 $n = < s, i > \in N$, 那么 $index(n) = i$, $strand(n) = s$. 如果 $(tr(s))_i = < \delta, a >$, 那么 $term(n) = +a$或 $term(n) = -a$; 对于术语 a, 用 $node(+a)$ 或 $node(-a)$ 表示它所在的结点.

(3) $n_1, n_2 \in N$, 那么 $n_1 \rightarrow n_2$ 表示 $term(n_1) = +a$, $term(n_2) = -a$.

(4) $n_1, n_2 \in N$, 那么 $n_1 \Rightarrow n_2$ 表示 n_1 和 n_2 属于同一个 *strand*, 且 $index(n_2) = index(n_1) + 1$.

(5)术语 t源发于结点 n当且仅当 $sign(n) = +$, $t \sqsubset term(n)$; 而且对于同一个 *strand* 上任何先于 n 的结点 n', $t \sqsubset term(n')$ 不成立.

(6)术语 t唯一源发于结点 n, 当且仅当存在唯一的结点 n, 术语 t源发于结点 n. 所以, *strand space* 构成一个有向图 (N, E), N 是结点集合, 边 $E = \rightarrow \cup \Rightarrow$.

定义 **4**　设 $C = (N_C, (\rightarrow_C \cup \Rightarrow_C))$, $\rightarrow_C \subset \rightarrow$, $\Rightarrow_C \subset \Rightarrow$, C 是 bundle, 如果满足下面的条件:

(1) C 是有限集;

(2)如果 $n_2 \in N_C$, 且 $sign(n_2) = -$, 那么有唯一 n_1, 满足 $n_1 \rightarrow_C n_2$;

(3)如果 $n_2 \in N_C$, 且有 $n_1 \Rightarrow n_2$, 那么 $n_1 \Rightarrow_C n_2$;

(4) C 是非循环的.

1.3 攻击者的迹

定义 **5** 攻击者的迹可为下列情况中的一种:

M. *TextMessage*: $< + t >$, 其中 $t \in T$;

F. *Flushing*: $< - g >$;

T. *Tee*: $< - g, + g, + g >$;

C. *Concatenation*: $< - g, - h, + gh >$;

S. *Separation into components*: $< - gh, + g, + h >$;

K. *Key*: $< + K >$, 其中 $K \in K_P$, K_P 是攻击者初始已知的密钥集合;

E. *Encryption*: $< - K, - h, + \{h\}_K >$;

D. *Decryption*: $< - K^{-1}, - \{h\}_K, + h >$.

2 Denning-Sacco密钥分配协议的攻击

2.1 协议描述

Denning-Sacco密钥分配协议[8]描述如下:

$$M_1 \quad A \rightarrow S: A, B$$

$$M_2 \quad S \rightarrow A: \{\{A, SK_A\}_{SK_S^{-1}}, \{B, SK_B\}_{SK_S^{-1}}\}$$

$$M_3 \quad A \rightarrow B: \{\{K_{ab}, T_1\}_{SK_A^{-1}}\}_{K_B}, \{A, SK_A\}_{SK_S^{-1}}, \{B, SK_B\}_{SK_S^{-1}}$$

在上述协议中, A 是协议的发起者, B 是协议的响应者, S 是认证服务器, SK_S^{-1} 是 S 的签名私钥, SK_A^{-1} 是 A 的签名私钥, K_B 是 B 的加密公钥, K 是 A 生成的共享密钥, T_1 是时戳. 协议完成后, 主体 A 和主体 B 共享密钥 K_{ab}.

2.2 Denning-Sacco密钥分配协议的攻击

第一种攻击方法:

$$M_1' \quad B(A) \rightarrow S: A, C$$

$$M_2' \quad S \rightarrow B(A): \{\{A, SK_A\}_{K_S^{-1}}, \{C, SK_C\}_{K_S^{-1}}\}$$

$$M_3' \quad B(A) \rightarrow C: \{\{K_{ab}, T_1\}_{SK_A^{-1}}\}_{K_C}, \{A, SK_A\}_{K_S^{-1}}, \{C, SK_C\}_{K_S^{-1}}$$

主体 A 和主体 B 首先进行了一轮协议, 主体 B 从主体 A 那里得到了 $\{K_{ab}, T_1\}_{SK_A^{-1}}$. 随后主体 B 伪装成主体 A 与主体 C 又进行了一轮协议, 使得 C 认为自己和主体 A 共享了密钥 K, 但主体 A 根本没有参与通信, 所以 B 攻击成功, 这是典型的重放攻击.

第二种攻击方法:

$$M_1'' \quad A \rightarrow S: A, B$$

$$M_2'' \quad S \rightarrow A: \{\{A, SK_A\}_{K_S^{-1}}, \{B, SK_B\}_{K_S^{-1}}\}$$

$$M_3'' \quad A \rightarrow Z(B): \{\{K_{ab}, T_1\}_{SK_A^{-1}}\}_{K_B}, \{A, SK_A\}_{K_S^{-1}}, \{B, SK_B\}_{K_S^{-1}}$$

在这个协议中, 第一、二条消息与原来的协议一样, 第三条消息本来是主体 A 发送给主体 B 的, 但是被攻击者 Z 截获了. 主体 A 以为自己已经和主体 B 共享了会话密钥 K, 但是实际上 B 并没有参与协议, 所以 Z 攻击成功.

3 Denning-Sacco密钥分配协议的改进

针对 Denning-Sacco密钥分配协议存在的上述攻击方式, 我们把协议修改为:

$$M_1''' \quad A \rightarrow S: A, B$$

$$M_2''' \quad S \rightarrow A: \{\{A, SK_A\}_{SK_S^{-1}}, \{B, SK_B\}_{SK_S^{-1}}\}$$

M_3'''　$A \rightarrow B$: $\{\{A, B, K_{ab}, T_1\}_{SK_A^{-1}}\}_{K_B}$, $\{A, SK_A\}_{SK_S^{-1}}$, $\{B, SK_B\}_{SK_S^{-1}}$

M_4'''　$B \rightarrow A$: $\{\{A, B, K_{ab}, T_1\}_{SK_A^{-1}}\}_{K_A}$

下面用串空间模型来证明修改后的协议能够达到协议需要完成的目标.

根据上述协议的描述, 我们知道在 Denning- Sacco密钥分配协议中共有三个主体, 即协议的发起者 A、协议的响应者 B 和认证服务器 S. 构造 Denning- Sacco密钥分配协议的串空间如下:

协议的发起者串为 $s_i \in Init[A, B, T_1, K_{ab}]$, 其迹为:

$< + \{A, B\}, - \{\{A, SK_A\}_{SK_S^{-1}}, \{B, SK_B\}_{SK_S^{-1}}\}, + \{\{\{A, B, K_{ab}, T_1\}_{SK_A^{-1}}\}_{K_B}, \{A, SK_A\}_{SK_A^{-1}}, \{B, SK_B\}_{SK_S^{-1}}\}, - \{\{A, B, K_{ab}, T_1\}_{SK_A^{-1}}\}_{K_A} >$

协议的响应者串为: $s_r \in Resp[A, B, T_1, K_{ab}]$, 其迹为:

$< - \{\{\{A, B, K_{ab}, T_1\}_{SK_A^{-1}}\}_{K_B}, \{A, SK_A\}_{SK_S^{-1}}, \{B, SK_B\}_{SK_S^{-1}}\}, + \{\{A, B, K_{ab}, T_1\}_{SK_A^{-1}}\}_{K_A} >$

认证服务器串为 $s_s \in Serv[A, B, T_1, K_{ab}]$, 其迹为:

$< - \{A, B\}, + \{\{A, SK_A\}_{SK_S^{-1}}, \{B, SK_B\}_{SK_S^{-1}}\} >$

Denning- Sacco密钥分配协议的串空间为:

$\sum = Init[A, B, T_1, K_{ab}] \cup Resp[A, B, T_1, K_{ab}] \cup Serv[A, B, T_1, K_{ab}] \cup P$,

其中 P 为攻击者的迹.

Denning- Sacco密钥分配协议需要证明的目标有三: 一是存在一个协议的发起者 *strand* t, 它的迹为 $Init[x, y, T_1, K_{ab}]$; 二是证明协议的发起者为 A, 即 $x = A$; 三是证明协议的响应者为 B, 即 $y = B$. 下面分为三个命题进行证明. 设 C是一个描述 Denning- Sacco密钥分配协议的 bundle, 见图 1.

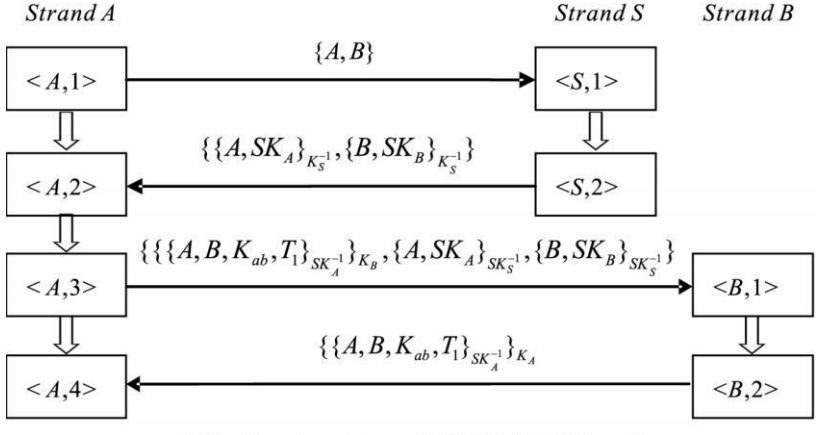

图1　Denning-Sacco密钥分配协议的bundle

Fig. 1　The bundle of Denning-Sacco key distribution with public key

命题 **1**　存在一个协议的发起者 *strand* t, 它的迹为 $Init[x, y, T_1, K_{ab}]$.

证明　构造集合 $F = \{n \mid n \in C \wedge K_{ab} \in term(n) \wedge K_{ab} \neq term(n)\}$, 从图 1可以看出集合 F 不空, 根据串空间的性质, F 必有 $\leqslant_C$ 最小元, 设为 m, $sign(m) = +$. 只需要证明 $m \notin P$ 和 $m \notin S$ 就可以了.

(1)证明 $m \notin P$, 只需要分别讨论攻击者的迹. 下面根据定义 5分别进行讨论:

M. 迹的形式为 $< + t >$, 其中 $t \in T$, 但是 $m \notin T$;

F. 迹的形式为 $< - g >$, 而 $sign(m) = +$;

T. 迹的形式为 $< - g, + g, + g >$, 没有源发于正结点的值;

C. 迹的形式为 $< - g, - h, + gh >$, 没有源发于正结点的值;

S. 迹的形式为 $< - gh, + g, + h >$, 没有源发于正结点的值;

K. 迹的形式为 $< + K >$, 其中 $K \in K_P$, K_P 是攻击者初始已知的密钥集合, 但 $m \notin K_P$;

E. 迹的形式为 $< - K, - h, + \{h\}_K >$, 因为 $SK_A^{-1} \notin K_P$, 所以 $\{h\}_K$ 不会被合法的主体接收;

D. 迹的形式为 *Decryption*: $< -K^{-1}, - \{h\}_K, + h >$, 若 $m = node(+ h)$, 那么 $K_{ab} \in h$, 所以有 $K_{ab} \in \{h\}_K$, 并且 $K_{ab} \neq \{h\}_K$, 这样 $node(- \{h\}_K) \in F$, 这和 m是最小元矛盾.

通过上面的分析可知, $m \notin P$.

(2)证明 $m \notin S$

由于认证服务器 S的迹为 $< - \{A, B\}, + \{\{A, SK_A\}_{SK_S^{-1}}, \{B, SK_B\}_{SK_S^{-1}}\} >$, $m \neq < S, 1 >$ 并且 $m \neq <$

$S, 2>$, 也就是 $m \notin S$.

由于 $m \notin P$, $m \notin S$, 而且 $m \notin Resp$, 只有 $m \in Init$, 也就是存在一个协议的发起者 strand t, 它的迹为 $Init[x, y, T_1, K_{ab}]$.

命题 **2** 证明协议的发起者为 A, 即 $x = A$.

证明 B 是根据 $\{A, B, K_{ab}, T_1\}_{SK_{\bar{A}}^{-1}}$ 来认证对方是否为 A, 构造集合 $G = \{n \mid \{A, B, K_{ab}, T_1\}_{SK_{\bar{A}}^{-1}} \in term(n) \wedge \{A, B, K_{ab}, T_1\}_{SK_{\bar{A}}^{-1}} \neq term(n)\}$, 因为 $<A, 3> \in G$, 所以 $G \neq \phi$, 根据串空间性质, G 必有最小元, 设为 m, $sign(m) = +$. 由于 SK_A^{-1} 是主体 A 的签名私钥, 只有 A 和 S 知道, 所以 $m \in Init$ 或者 $m \in Serv$. 因为 S 没有发送 $\{A, B, K_{ab}, T_1\}_{SK_{\bar{A}}^{-1}}$ 给 B, 所以 $m \notin Serv$. 这样只有 $m \in Init$ 即证明了 $x = A$.

命题 **3** 证明协议的响应者为 B, $y = B$.

证明 协议发起者的迹为:

$$<+\{A, B\}, -\{\{A, SK_A\}_{SK_{\bar{S}}^{-1}}, \{B, SK_B\}_{SK_{\bar{S}}^{-1}}\}, +\{\{\{A, B, K_{ab}, T_1\}_{SK_{\bar{A}}^{-1}}\}_{K_B}, \{A, SK_A\}_{SK_{\bar{S}}^{-1}}, \{B, SK_B\}_{SK_{\bar{S}}^{-1}}\}, -\{\{A, B, K_{ab}, T_1\}_{SK_{\bar{A}}^{-1}}\}_{K_A}>$$

根据 $\{A, B, K_{ab}, T_1\}_{SK_{\bar{A}}^{-1}}$ 的来源来判断协议的响应者是否为 B, 构造集合 $N = \{n \mid \{A, B, K_{ab}, T_1\}_{SK_{\bar{A}}^{-1}} \in term(n) \wedge \{A, B, K_{ab}, T_1\}_{SK_{\bar{A}}^{-1}} \neq term(n)\}$, $<B, 2> \in N$ 和 $<A, 3> \in N$, 所以 $N \neq \phi$, 根据串空间性质, N 必有最小元, 设为 m, $sign(m) = +$, 这里 $m = <A, 3>$. $\{A, B, K_{ab}, T_1\}_{SK_{\bar{A}}^{-1}}$ 是 A 用 B 的公钥加密后发送给 B 的, 只有 B 能得到. 现在 A 又收到了 $\{A, B, K_{ab}, T_1\}_{SK_{\bar{A}}^{-1}}$, 那肯定是 B 发送的, 也就是协议的响应者 $y = B$.

综上所述, 修改后的 Denning- Sacco密钥分配协议达到了协议需要达到的目标.

4 结束语

安全协议的分析问题, 是一个比较困难的问题, 也是当今国内国外研究得比较热的一个问题, 安全协议分析的研究具有重要的理论研究意义和实际意义. 本文首先对串空间模型进行了详细的介绍, 然后给出了对 Denning- Sacco密钥分配协议的两种攻击方式并对 Denning- Sacco密钥分配协议进行了修改. 利用串空间模型来对修改后的 Denning- Sacco密钥分配协议进行了分析, 发现修改后的协议能够抵抗本文中提到的两种攻击, 能顺利地完成协议的目标.

参考文献:

[1] Michael Burrows, Martín Abadi, Roger Needham. A logic of authentication[J]. ACM Transactions on Computer Systems, 1990, 8(1): 18- 36.

[2] Lowe G. Breaking and fixing the Needham- Schroeder public- key protocol using FDR[A]. In: Proc. TACAS, 1996: 147- 166.

[3] Paulson L C. The inductive approach to verifying cryptographic protocols[J]. Journal of Computer Security, 1998, 6: 85- 128.

[4] Javier Thayer Fábrega F, Jonathan C Herzog, Joshua D Guttman. Strand spaces: Why is a security protocol correct? [A]. In: Proceedings of the 1998 IEEE Symposium on Security and Privacy. Los Alamitos: IEEE Computer Society Press, 1998: 160- 171.

[5] Javier Thayer Fábrega F, Jonathan C Herzog, Joshua D Guttman. Strand spaces: Proving security protocols correct[J]. Journal of Computer Security, 1999, 7(2- 3): 191- 230.

[6] Javier Thayer Fábrega F, Jonathan C Herzog, Joshua D Guttman. Strand spaces: Honest ideals on strand spaces[A]. In: Proceedings of the 1998 IEEE Computer Security Foundations Workshop. Los Alamitos: IEEE Computer Society Press, 1998: 66- 77.

[7] Joshua D Guttman, Javier Thayer Fábrega F. Authentication tests[A]. In: Proceedings of the 2000 IEEE Symposium on Security and Privacy. Los Alamitos: IEEE Computer Society Press, 2000: 150- 164.

[8] Clark J, Jacob J. A Survey of Authentication Protocol Literature: Version 1.0[DB/OL]. Available via http://www.cs.york.ac.uk/jac/papers/drareview.ps.gz.