基于串空间和状态转换的认证协议分析方法*)

邓淼磊[1,2] 邱 罡[1] 周利华[1]
(西安电子科技大学 CNIS 教育部重点实验室 西安 710071)[1]
(解放军信息工程大学数学物理系 郑州 450001)[2]

摘 要 串空间是一种新兴的安全协议形式化分析模型。串空间模型中的理论证明方法虽然严谨,但难度很大。本文基于串空间模型,首先定义系统状态,并以 Needham-Schroeder-Lowe 公钥认证协议为例说明系统状态转换的分析过程。通过对状态转换过程中现实的跟踪考察,得出了有意义的结论。结合串空间模型,验证了该认证协议的安全性。这种分析认证协议的新方法简洁和高效,并易于实现自动化。

关键词 串空间,认证协议,状态转换,现实

Analysis of Authentication Protocols Based on Strand Space and State Transition

DENG Miao-Lei[1,2] QIU Gang[1] ZHOU Li-Hua[1]
(The CNIS Key Laboratory of the Education Ministry, Xidian University, Xi'an 710071)[1]
(Department of Mathematics and physics, The PLA Information Engineering University, Zhengzhou 450001)[2]

Abstract Strand space is a new formal model for the analysis of security protocols. Precise though they are, theory testifies in the strand space model are difficult. Firstly, based on the strand space model, the state of system is defined. Secondly, analysis process of transitions between system states is explained by the example of Needham-Schroeder-Lowe public key authentication protocol. Investigating nonces in transitions between system states, we draw some significant conclusions. Finally, the security of Needham- Schroeder-Lowe protocol is validated. This new method for analyzing authentication protocols is simple and efficient, and it is prone to be automated.

Keywords Strand space, Authentication protocol, State transition, Nonce

1 引言

认证协议使用密码技术,实现网络环境下的身份认证和信息保密。它看似简单,但若确保正确是极其困难的[1]。因此,对认证协议安全性进行分析就显得十分重要。当前,形式化的分析方法被公认为分析认证协议的最有效手段。

1998 年,Fabrega、Herzog 和 Guttman 提出了协议的串(Strand)空间模型[2],并应用该理论证明了 Needham-Schroeder-Lowe 公钥认证协议的正确性。串空间模型是一个有多方面优点的安全协议形式化分析方法:(1)可以进行基本的协议正确性证明[3];(2)通过引入入侵者串,能找出攻击方法[4];(3)可以给出基于串空间模型的协议设计方法[5]。由于其功能的全面性,对串空间方法的研究得到了较大的发展。

串空间模型的理论证明方法虽然严谨,但要依赖于专家的努力才能做到,难度很大,实用性差。

本文基于串空间模型,提出了一种高效的认证协议分析方法。首先把协议的执行环境看作一个系统,给出了系统状态的形式化定义。然后以 Needham-Schroeder-Lowe 公钥认证协议为例,对协议状态转换过程进行分析。这里注意到:由于在网络系统中很难保持全局统一的时钟,因此在认证协议中往往使用被称为"现时"(nonce)[6]的一段随机数,来保证通信双方每次会话的新鲜性。本文在协议的状态转换分析中,就是通过对现实的考察,得出了有意义的结论。最后结合串空间模型,实现了对该认证协议安全性的验证。本文验证协议安全性的过程简洁高效,并为协议验证的自动化实现提供了思路。

2 串空间模型

串空间模型借助于图论的方法描述协议的执行过程[7],它对协议安全性的分析方法类似于归纳法[8]。串空间模型能够准确描述协议执行过程中事件的先后顺序关系,为研究人员提供了一种全新的协议分析方法。

2.1 基本概念

串是协议主体可能参与的一个接收和发送消息的事件序列。对于一个诚实主体(即严格按照协议规则执行的主体),它表示在协议的一次特定运行中主体的行为,不同主体的行为用不同的串表示。入侵者的串是入侵者可能发送和接收的消息序列,它模拟入侵者假定具有的能力。

考虑这样一个集合 M,它的元素就是某个协议中主体之间交换的所有可能的消息。我们称 M 的元素为项。在一个协议中,主体可以接收或发送项。在这里项以带正号的形式出现时表示发送一条消息,以带负号的形式出现时表示接收一条消息。

定义 1 一个有符号项是一个二元组$\langle\sigma,a\rangle$,其中$a\in M$,σ是+号或−号。

这样可以把一个有符号项记作$+a$或$-a$。$(\pm M)^*$表示有符号项的有限序列的集合。定义迹为一个有符号项的有限序列。

*)本课题得到解放军信息工程大学重点研究方向基金资助。邓淼磊 博士生、讲师,主要研究领域为网络信息安全;邱 罡 博士生、讲师,主要研究领域为网络信息安全;周利华 博士、教授、博士生导师,主要研究领域为计算机网络安全理论与技术、多媒体技术等。

定义 2 M 上的一个串空间是一个串的集合 Σ，存在一个迹的映射 $tr:\Sigma\rightarrow(\pm M)^*$。

定义 3 对于一个串空间 Σ，结点是一个序偶 $\langle e,i\rangle$，其中 $e\in\Sigma$，i 是满足 $1\leqslant i\leqslant$length(tr(s))的整数。称结点 $d=\langle e,i\rangle$ 属于串 s 或在串 s 上，记作 $d\in s$。显然，每一个结点都属于唯一的一条串。

串空间模型中的另一个重要概念是束(bundle)。束是一个在因果关系上闭合的结点集合。这意味着如果束中的一个结点在某条串上，那么它在同一条串上的前继结点也在该束中。如果一个消息接收结点在一个束中，那么相应的消息发送结点也在该束中。

2.2 入侵者串

入侵者可用的原子操作被嵌入到一个入侵者串的集合中。它们概括了入侵者的能力：生成文本消息(例如主体名称、新的现实等)，连接、分离、重放或删除消息，使用入侵者可用的密钥进行密码操作等。入侵者对协议进行攻击时一般需要把这些原子操作中的某几个结合起来。

2.3 安全属性的表示

Gavin Lowe 研究了一系列认证属性[9]；串空间模型非常适合陈述和验证他提出的一致(Agreement)属性。协议的一致属性有两个层次：

(1)强一致属性。协议保证主体 B(假定作为响应者)在某些数据项 x 上与另一主体 A(假定作为发起者)达成一致，如果：每次 B 作为响应者使用数据 x 与他所认为的 A(发起者)完成一轮协议执行时，确实存在唯一的一轮协议执行，其中 A 作为发起者也使用 x，并且认为他的响应者为 B。

(2)弱一致属性。每次 B 作为响应者使用数据 x 与他所认为的 A(发起者)完成一轮协议执行时，确实存在一轮协议执行，其中 A 作为发起者也使用 x，并且认为他的响应者为 B。

两者的区别是弱一致属性不能保证协议执行的唯一性，即不能保证主体 B 的每轮执行与主体 A 的每轮执行之间的一一对应关系。它不能防止 A 执行了多轮与 B 对应的协议，而 B 只执行了一轮。类似地，对于发起者也存在同样的一致性条件。

可以用如下方法验证弱一致属性：只要束 C 中包含一条使用 x 的响应者串，那么 C 中也就包含一条使用 x 的发起者串。也可以通过说明 C 中包含一条唯一的使用 x 的发起者串来验证强一致属性。

3 系统状态的定义

定义 4 系统的状态由发送或接收的消息集合 M 和协议主体的状态集合 S 来表征。其中集合 S 的元素记作 $p:s$，这里 p 是一个主体，s 是 p 的一个状态。称序偶 $\langle M,S\rangle$ 为一个系统状态。

用 $N(M,S)$ 表示协议执行过程中主体生成的现实的集合。

定义 5 协议的每步执行是下列两种操作或仅是第一种操作：①接收一条消息 $m\in M$ 或发送一条消息 $m'\in M$；②生成一个现实 $n\in N(M,S)$。

对于某一主体 p，状态 $p:s\in S$，其对协议的每一步执行都可以看作是两个系统状态之间的转换。主体 p 转换后的状态用 $p:s'$ 表示。

假设 $\langle M,S\rangle$ 为初识的系统状态，p 执行单步协议后，系统将转换到如下状态：$\langle M\cup\{m'\},(S-\{p:s\})\cup\{p:s'\}\rangle$。

定义 6 系统状态间的转换关系$\rightarrow$定义为：

$\forall p:s\in S,\forall m\in M,\forall n\in N(M,S)$，执行单步协议后，$\langle M,S\rangle\rightarrow\langle M\cup\{m'\},(S-\{p:s\})\cup\{p:s'\}\rangle$。

关系$\rightarrow$的自反、传递闭包记为$\rightarrow^*$。

4 系统状态转换分析

这里以 Needham-Schroeder-Lowe 公钥协议为例说明状态转换分析过程。这个协议由 Lowe 提出[10]以弥补 Needham 和 Schroeder 提出的公钥协议[11]的缺陷。根据串空间思想，协议图示如图 1。

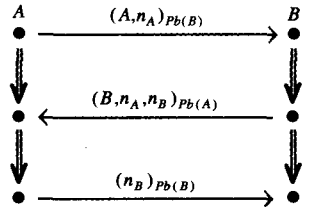

图 1 Needham-Schroeder-Lowe 协议

这里 $Pb(A)$ 和 $Pb(B)$ 分别表示主体 A 和 B 的公钥。

本文用集合 $I(M,S)$ 表示入侵者能够生成的消息的集合。根据串空间模型，集合 $I(M,S)$ 的元素包括 M、由 M 分解的消息、导入的现实，以及由此合成的消息。

对于 Needham-Schroeder-Lowe 协议，系统状态转换关系$\rightarrow$可以定义如下：

转换①入侵者发送消息 m：此时 $m\in I(M,S)$；$\langle M,S\rangle\rightarrow\langle M\cup\{m\},S\rangle$。

转换②A 发送消息 $(A,n_A)_{Pb(B)}$：此时 $n_A\in N(M,S)$；$\langle M,S\rangle\rightarrow\langle M\cup\{A,n_A\}_{Pb(B)},S\cup\{A:s_0(B,n_A)\}\rangle$。

转换③B 发送消息 $(B,n_A,n_B)_{Pb(A)}$：此时 $(A,n_A)_{Pb(B)}\in M,n_B\in N(M,S)$；$\langle M,S\rangle\rightarrow\langle M\cup\{(B,n_A,n_B)_{Pb(A)}\},S\cup\{B:s_1(A,n_A,n_B)\}\rangle$。

转换④A 发送消息 $(n_B)_{Pb(B)}$：此时 $(B,n_A,n_B)_{Pb(A)}\in M$，$A:s_0(B,n_A)\in S$；$\langle M,S\rangle\rightarrow\langle M\cup\{(n_B)_{Pb(B)}\},(S-\{A:s_0(B,n_A)\})\cup\{A:s_2(B,n_A,n_B)\}\rangle$。

转换⑤B 接收消息 $(n_B)_{Pb(B)}$：此时 $(n_B)_{Pb(B)}\in M,B:s_1(A,n_A,n_B)\in S$；$\langle M,S\rangle\rightarrow\langle M,(S-\{B:s_1(A,n_A,n_B)\})\cup\{B:s_3(A,n_A,n_B)\}\rangle$。

在上述转换关系中，s_0，s_1，s_2 和 s_3 为状态构造符。

对转换③中引入的现实 n_B 进行分析，得到下面的引理。

引理 1 假设由转换③$\langle M,S\rangle\rightarrow\langle M_1,S_1\rangle$ 成立，即，$(A,n_A)_{Pb(B)}\in M,n_B\in N(M,S)$，$M_1=M\cup\{(B,n_A,n_B)_{Pb(A)}$，$S_1=S\cup\{B:s_1(A,n_A,n_B)\}$。则对于 $\langle M_1,S_1\rangle\rightarrow^*\langle M',S'\rangle$，下面两式总成立：

(1)如果 $m\in M'$ 且 m 包含 n_B，那么 $m=(B,n_A,n_B)_{Pb(A)}$ 或者 $m=(n_B)_{Pb(B)}$。

(2)如果 $s\in S'$ 且 s 包含 n_B，那么 $s=B:s_1(A,n_A,n_B)$，或者 $s=A:s_2(B,n_A,n_B)$，或者 $s=B:s_3(A,n_A,n_B)$。

证明：在$\rightarrow^*$上进行归纳证明。如果 $\langle M',S'\rangle=\langle M_1,S_1\rangle$，结论显然成立。

假设它们对于 $\langle M',S'\rangle$ 成立，而 $\langle M',S'\rangle,\rightarrow\langle M'',S''\rangle$，下面根据系统的五种状态转换分别分析。

转换① 根据假设，如果 $m'\in M'$ 且 m' 包含 n_B，那么 $m'=(B,n_A,n_B)_{Pb(A)}$ 或者 $m'=(n_B)_{Pb(B)}$。由于入侵者不知道 A 和

B 的私钥，它不能从 $(B,n_A,n_B)_{Pb(A)}$ 或 $(n_B)_{Pb(B)}$ 中得到 n_B。因此，即使 $m'\in I(M',S')$，也有 $m'=(B,n_A,n_B)_{Pb(A)}$ 或 $m'=(n_B)_{pb(B)}$。所以(1)式成立。因为 $S''=S'$，(2)式也成立。

转换② 如果 $n_{A'}\in I(M',S')$，由于 n_B 在 M' 中，$n_{A'}\neq n_B$，因此 $(A',n_{A'})_{Pb(B')}$ 和 $A':s_0(B',n_{A'})$ 都不包含 n_B。两式都成立。

转换③ 根据假设，$(A',n_{A'})_{pb(B')}$ 不包含 n_B。如果 $n_{B'}\in N(M',S')$，那么 $n_{B'}\neq n_B$。因此，$(B',n_{A'},n_{B'})_{Pb(A')}$ 和 $B':s_1(A',n_{A'},n_{B'})$ 都不包含 n_B。两式都成立。

转换④ 根据 $(B',n_{A'},n_{B'})_{Pb(A')}$ 是否包含 n_B 分别分析。如果 $n_B\in(B',n_{A'},n_{B'})_{Pb(A')}$，根据假设，$(B',n_{A'},n_{B'})_{Pb(A')}=(B,n_A,n_B)_{Pb(A)}$。因此转换前 A 的状态是 $A:s_0(B,n_A)$。发送消息 $(n_B)_{Pb(B)}$ 后，A 的状态也成为 $A:s_2(B,n_A,n_B)$。这就隐含了引理的两条结论。

如果 $(B',n_{A'},n_{B'})_{Pb(A')}$ 不包含 n_B，$A':s_0(B',n_{A'})$ 也不包含 n_B。因此 $(n_{B'})_{Pb(B')}$ 和 $A':s_2(B',n_{A'},n_{B'})$ 都不包含 n_B。两式也都成立。

转换⑤ 根据 $(n_{B'})_{Pb(B')}$ 是否包含 n_B 分别分析。如果 $n_B\in(n_{B'})_{Pb(B')}$，则 $(n_{B'})_{Pb(B')}=(n_B)_{Pb(B)}$。因此状态转换前 B 的状态形式是 $B:s_1(?,?,n_B)$。由于 $B:s_1(?,?,n_B)$ 包含 n_B，根据假设，$B:s_1(?,?,n_B)=B:s_1(A,n_A,n_B)$。因此转换后的状态是 $B:s_3(A,n_A,n_B)$。

如果 $(n_{B'})_{Pb(B')}$ 不包含 n_B，那么 $B':s_1(A',n_{A'},n_{B'})$ 不包含 n_B。这是因为如果 $B':s_1(A',n_{A'},n_{B'})$ 包含 n_B，根据假设，$B':s_1(A',n_{A'},n_{B'})=B:s_1(A,n_A,n_B)$，且 $(n_{B'})_{Pb(B')}=(n_B)_{Pb(B)}$。出现矛盾。

证毕。

对转换②中引入的现实 n_A 进行分析，可以得到下面的引理。

引理 2 假设由转换②$\langle M,S\rangle\rightarrow\langle M_1,S_1\rangle$ 成立，即，$n_A\in N(M,S)$，$M_1=M\cup\{(A,n_A)_{Pb(B)}\}$，$S_1=S\cup\{A:s_0(B,n_A)\}$。则对于 $\langle M_1,S_1\rangle\rightarrow^*\langle M',S'\rangle$，下面两式总成立：

(1)如果 $m\in M'$ 且 m 包含 n_A，那么对于某 X，$m=(A,n_A)_{Pb(B)}$ 或者 $m=(B,n_A,X)_{Pb(A)}$。

(2)如果 $s\in S'$ 且 s 包含 n_A，那么对于某 X，$s=A:s_0(B,n_A)$，或者 $s=B:s_1(A,n_A,X)$，或者 $s=A:s_2(B,n_A,X)$，或者 $s=B:s_3(A,n_A,X)$。

它的证明过程与引理 1 类似。

这两个引理的意义在于：如果一个主体到达系统的某一状态，可以推断出只能是协议合法运行的结果。假设主体 B 按照转换⑤改变状态到 $s_3(A,n_A,n_B)$，由转换③可知 B 之前在状态 $s_1(A,n_A,n_B)$。根据引理 1，只有 A 和 B 知道随机数 n_B，并且只有 A 能生成消息 $(n_B)_{Pb(B)}$。这表明 A 之前在状态 $s_2(B,n_A,n_B)$。类似地，如果 A 改变状态到 $s_2(B,n_A,n_B)$，则 B 之前在状态 $s_1(A,n_A,n_B)$ 并且生成消息 $(B,n_A,n_B)_{Pb(A)}$。

5 协议安全性验证

Needham-Schroeder-Lowe 协议的串空间 Σ 是如下三种串的组合：

(1)入侵者串；

(2)发起者串 $t\in\mathrm{Init}[A,B,n_A,n_B]$，具有迹 $\langle+(A,n_A)_{Pb(B)},-(B,n_A,n_B)_{Pb(A)},+(n_B)_{Pb(B)}\rangle$；

(3)响应者串 $r\in\mathrm{Resp}[A,B,n_A,n_B]$，具有迹 $\langle-(A,n_A)_{Pb(B)},+(B,n_A,n_B)_{Pb(A)},-(n_B)_{Pb(B)}\rangle$。

分别称 A 和 B 为协议发起者和响应者。任给 Σ 中的一条串，能够仅根据其迹的形式把它唯一地归类为一条入侵者串、发起者串或响应者串。

响应者 B 的弱一致属性可表述为下面的命题。

命题 1 Σ 是本协议的串空间，C 是包含一条响应者串 $r\in\mathrm{Resp}[A,B,n_A,n_B]$ 的束，$n_A\neq n_B$，n_B 唯一生成于 Σ 中，A 的私钥没有泄露。那么 C 包含一条发起者串 $t\in\mathrm{Init}[A,B,n_A,n_B]$。

证明：由上节最后的分析，可知相应于 $-(n_B)_{Pb(B)}$ 的结点不是入侵者结点，因此存在一个发起者结点 $+(n_B)_{Pb(B)}$。于是得到发起者串的迹 $\langle+(A',n'_A)_{Pb(B)},-(B,n'_A,n_B)_{Pb(A')},+(n_B)_{Pb(B)}\rangle$。

根据引理 1 和上节最后的分析，因为 $(B,n'_A,n_B)_{Pb(A')}$ 包含 n_B，唯一的相应于 $-(B,n'_A,n_B)_{Pb(A')}$ 的结点是响应者的结点 $+(B,n_A,n_B)_{Pb(A)}$。因此 $A'=A,n'_A=n_A$。即发起者串的迹为 $\langle+(A,n_A)_{Pb(B)},-(B,n_A,n_B)_{Pb(A)},+(n_B)_{Pb(B)}\rangle$。证毕。

又根据现实 n_A 的唯一性，响应者的强一致属性也就得到了保证。

发起者 A 的一致属性可表述为下面的命题。

命题 2 Σ 是本协议的串空间，C 是包含一条发起者串 $t\in\mathrm{Resp}[A,B,n_A,n_B]$ 的束，n_A 唯一生成于 Σ 中，A 和 B 的私钥没有泄露。那么 C 包含一条至少含有初始两个结点的响应者串 $r\in\mathrm{Init}[A,B,n_A,n_B]$。

它的证明过程与命题 1 类似。

结论 本文提出了一种基于串空间模型和系统状态转换分析的认证协议分析验证方法。用这种方法对 Needham-Schroeder-Lowe 协议的安全性进行了验证，得出了与文[2]相同的结论。本文对协议安全性的验证与原始的串空间模型中的推导过程相比，要简单和高效。另外，由于对系统状态转换的分析可以实现自动化，束的构造也可以自动化[12]，由此可以设计一个非常强大且简单高效的协议自动验证工具。

参 考 文 献

1 Lowe G. An attack on the needham-schroeder public key authentication protocol[J]. Information Processing Letters, 1995, 56(3):131～136

2 Thayer F, Herzog J C, Guttman J D. Strand space: why is a security protocol correct[C]. In: Proceedings of the 1998 IEEE Symposium on Security and Privacy. IEEE Computer Society Press, 1998(5):160～171

3 Thayer F, Herzog J C, Guttman J D. Strand spaces: proving security protocols Correct[J]. Journal of Computer Security, 1999, 7(2):191～230

4 Liu Dongxi, Li Xiaoyong, Bai Yingcai. An attact-finding algorithm for security protocols[J]. Journal of Computer Science and Technology, 2002, 17(4):450～563

5 Guttman J D. Security protocol design via authentication tests [C]. In: Proceedings 15th IEEE Computer Security Foundations Workshop(CSFW-15), IEEE Computer Society Press, 2002. 92～103

6 Burrows M, Abadi M, Needham R. A logic of authentication[J]. ACM Transactions on Computer System, 1990, 8(1):18～36

7 Thayer F, Herzog J C, Guttman J D. Strand space picture[C]. In: the LICS Workshop on Formal Methods and Security Protocols, 1998

8 Paulson L C. The inductive approach to verifying cryptographic protocols[J]. Journal of Computer Security, 1998,6(1):85～128

9 Lowe G. A hierarchy of authentication specifications[C]. In:10th Computer Secutity Foundations Workshop Proceedings, IEEE Computer Society Press, 1997. 31～43

10 Lowe G. Breaking and fixing the needham-schroeder public-key protocol using FDR[C]. In: Proceedings of TACAS, Springer Verlag, 1996. 147～166

11 Needham R M, Schroeder M D. Using encryption for authentication in large networks of computers[J]. Communications of the ACM, 1978, 21(12):993～999

12 Song D X. Athena: A new efficient automated checker for security protocol analysis[C]. In: Proceedings of the 12th IEEE Computer Security Foundations Workshop, IEEE Computer Society Press, 1999