基于串空间模型安全协议形式化分析方法的研究

董 军,杨秀娟,赵艳芹
(黑龙江科技学院 计算机与信息工程学院,黑龙江 哈尔滨 150027)

摘 要:从串空间模型理论入手,提出了三种典型的串空间形式化方法(基于极小元理论的串空间方法、基于理想与诚实理论的串空间方法、基于认证测试理论的串空间方法),并对每一种方法的证明步骤及优缺点进行了分析。在此基础上,应用提出的串空间方法对 Yahalom 协议的秘密性和认证性进行了分析。分析结果表明利用不同方法的优点,能更好地保证安全协议形式化分析的准确性。

关键词:串空间;安全协议;认证测试
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2008)04-0151-04

Research on Formalisms Analysis Method Based on Strand Space Model Security Protocol

DONG Jun, YANG Xiu-juan, ZHAO Yan-qin
(Department of Computer & Information Engineering, Heilongjiang Institute of Science and Technology, Harbin 150027, China)

Abstract: Starting with the theory of strand space model, presents three typical formalisms based on strand space model, including the strand space method based on the minimal theory, the strand space method based on the honest ideal theory and the strand space method based on the authentication test theory. Moreover, also analyses the process of verification, advantages and flaws of these methods. Finally, using the proposed methods, Yahalom protocol is analysed from the aspects of both secrecy and authentication. Experimental results show that utilizing the advantage of various formalisms can greatly ensure the accuracy of formal analysis.

Key words: strand space; security protocol; authentication test

0 引 言

目前,基于不变集的代数定理证明方法是安全协议形式化分析领域研究的热点和难点问题,在这类方法中以串空间模型最为著名。串空间模型[1]由 Thayer, Herzog 和 Guttman 三人提出,该模型吸纳了 NRL 协议器、Schneider 秩函数和 Paulson 归纳法等方法的思想,并将协议的描述和目标安全属性都转化为图结构,有利于借助图的理论和算法进行协议安全性分析。

近些年已有一些国内外的学者、专家研究串空间模型,并将此模型用于安全协议的分析中,同时也针对某一类协议提出了一些行之有效的方法。但是这些方法是零散的、不成体系的。

文中首先给出了在串空间模型内认证协议正确性的含义并将其以逻辑公式的形式总结出来;其次从基于串空间模型的形式化分析方法所应用的理论知识入手,提出了基于极小元理论的串空间方法、基于理想与诚实理论的串空间方法和基于认证测试理论的串空间方法。

收稿日期:2007-07-04
基金项目:黑龙江省自然科学基金(CF2005-05)
作者简介:董 军(1976-),男,黑龙江肇东人,讲师,硕士,研究领域为计算机网络与信息安全。

1 串空间模型内协议正确性的含义

对于认证协议来讲,串空间模型将其安全目标规约为认证性和秘密性[2]。

(1)认证性。将协议 P 对 B(扮演响应者角色)使用向量参数 x 实现了认证性描述如下:任何时候 B 作为响应者(B 认为他在和 A 进行会话)使用 x 完成了一轮协议;则必定存在唯一的一轮协议,在这轮协议中 A 使用相同的 x 发起了一次会话,且 A 认为他是在与 B 进行会话。

假定 $\phi(s)$ 表示串的类型,$\varphi(s,s')$ 表示与 s 拥有共享密钥串 s' 的类型,则认证性的证明可表示成逻辑公式 F:

$$\forall C \forall s \exists s'.C\_\ \text{height}(s) = i \wedge \phi(s) \Rightarrow C\_$$

$\text{height}(s') = j \wedge \varphi(s, s')$

(2) 秘密性。假设 W 是所有包含消息 v 的串的集合(v 与 W 中的任一串的某个结点的消息项之间存在着子项关系),消息 v 在协议中的保密性描述如下:在任意包含 W 的丛 C 中,攻击者不能够直接接收到消息 v,也有能够通过他掌握的密钥集合 K_p 解密已接收的任一消息项来得到消息 v。假定 K 是所有密钥的集合,K 是严格安全密钥集($K \cap K_p = \varnothing$),令集合 $S = \{v\} \cup K$,$k = K/S$,$\phi(s)$ 表示串的类型,则秘密性被表示成如下的逻辑公式 F:

$$\forall C \forall s \forall n. \phi(s) \wedge n \in C \Rightarrow \text{term}(n) \notin I_k[S]$$

2 安全协议形式化分析的理论基础

2.1 理想与诚实理论

定义 1 如果 $k \subseteq K$,I 是消息空间 A 上的一个子集,如果 I 满足:对于任意的 $h \in I$,$g \in A$ 以及 $k \in K$,有 ①$hg, gh \in I$;②$\{h\}_k \in I$,则称 I 是 A 的一个 k - 理想,包含 h 的最小 k - 理想表示为 $I_k[h]$,如果 $S \subseteq A$,则 $I_k[S]$ 表示包含 S 的最小 k - 理想,且

$$I_k[h] = \bigcup_{x \in S} I_k[x]$$

定义 2 假设 C 是 A 上的丛,$I \subseteq A$,则 I 是诚实的当且仅当若 I 的入口点中有攻击者结点 p,则 p 是 M 结点或 K 结点。

2.2 认证测试理论

(1)基本概念。

定义 3 项 t_0 是 t 的组件,当且仅当 $t_0 \subset t$,t_0 不属于级联类型,并且对于任意 $t_1 \neq t_0$,如果有 $t_0 \subset t_1 \subset t$,那么,$t_1$ 属于级联类型。消息组件或者是原子数据类型,或者是加密类型。

定义 4 设 $a \in A$,n_1 和 n_2 为同一个串中的结点,则边 $n_1 \Rightarrow^+ n_2$ 是关于值 a 的被转换边当且仅当 a 在结点 n_1 发送,并在结点 n_2 从新组件中接收;边是 $n_1 \Rightarrow^+ n_2$ 关于值 a 的转换边当且仅当 a 在结点 n_1 接送,并在结点 n_2 存在于新组件中发送。

定义 5 $t = \{h\}_k$ 是结点 n 关于 a 的测试组件,则

①$a \subset t$,并且 t 是结点 n 的组件;

②t 不是串空间中任意其它正常结点的组件的子项。

(2) 三种认证测试方法。

方法 1 边 $n_1 \Rightarrow^+ n_2$ 是项 $t = \{h\}_k$ 关于值 a 的输出认证测试,如果:

① 边 $n_1 \Rightarrow^+ n_2$ 是 a 的一个测试;

②$k^{-1} \notin K_p$;

③a 不在结点 n_1 的除 t 以外的任何其它组件中出现;

④t 是结点 n_1 关于 a 的一个测试组件。

方法 2 边 $n_1 \Rightarrow^+ n_2$ 是项 $t = \{h\}_k$ 关于值 a 的输入认证测试,如果:

① 边 $n_1 \Rightarrow^+ n_2$ 是 a 的一个测试;

②$k \notin K_p$;

③t 是结点 n_1 关于 a 的一个测试组件。

方法 3 负结点 n 是项 $t = \{h\}_k$ 关于值 a 的主动认证测试,如果:

①t 是结点 n 关于 a 的一个测试组件;

②$k \notin K_p$。

(3) 三种认证测试规则。

规则 1 假设 C 是某协议串空间的一个丛,结点 $n' \in C$,边 $n \Rightarrow^+ n'$ 是项 t 关于值 a 输出认证测试,则

①必然存在结点 m,$m' \in C$ 满足 t 是 m 的消息组件,并且边 $m \Rightarrow^+ m'$ 是值 a 的转换边。

② 如果假设 a 只在结点 m' 的组件 $t_1 = \{h_1\}_{k_1}$ 中出现,t_1 不是任何其它正常结点的子项,并且 $k_1^{-1} \notin K_p$,那么必然存在一个包含 t_1 为组件的正常结点(负结点)。

规则 2 假设 C 是某协议串空间的一个丛,结点 $n' \in C$,边 $n \Rightarrow^+ n'$ 是项 t' 关于值 a 的输入认证测试,则必然存在结点 m,$m' \in C$ 满足 t' 是 m' 的消息组件,并且边 $m \Rightarrow^+ m'$ 是值 a 的转换边。

规则 3 假设 C 是某协议串空间的一个丛,结点 $n \in C$,n 是项 $t = \{h\}_k$ 的主动认证测试,则必然存在一个常规发送结点 $m \in C$ 满足 t 是 m 的消息组件。

3 安全协议的形式化分析方法

3.1 基于极小元理论的串空间方法

这种方法是串空间模型早期的一种典型的证明方法,其证明思路是:

(1)首先在丛中根据需要构造一个结点集,并考查这个集合中的极小元,判定它们是正则结点,还是攻击者结点。

(2)最后考察攻击者串的不同形式。

如在 NSL 协议的安全性证明中,为了证明响应者的认证性,首先构造集合 $S = \{n \in C: N_b \subset \text{term}(n) \wedge v_0 \not\subset \text{term}(n)\}$,通过考查 S 集合非空及 NSL 协议串空间的结点关系,可证明在集合 S 上存在一个关系 $\leq$ 的极小元 n_2 且 $\text{sign}(n_2) = +$,然后依次考查攻击者结点的各种可能情形,进而证明 n_2 不可能在一个攻击者串上。

基于极小元理论的串空间方法是有效的,但是这

种方法的缺陷也是较为明显的:在分析安全协议的安全特性,尤其是认证特性时,具有很高的技巧性。对于不同的安全协议,需要根据其具体的串空间图,选择不同的考察思路。并且对于安全协议中某些项的一些特性,如密钥的新鲜性,利用基于极小元理论的串空间方法不便于进行分析[3]。

3.2 基于理想与诚实理论的串空间方法

(1)协议秘密性分析。

基于理想与诚实理论分析协议秘密性思路是:

① 首先构造理想 $I_k[S]$,其中 S 是包含协议运行过程中需要保密的信息,而 k 中包含的是攻击者可能知道的密钥。其实所构造的 $I_k[S]$ 就是所有需要保密的消息用攻击者可能知道的密钥处理后的消息的集合。

② 应用诚实理论证明 $I_k[S]$ 是诚实的,若 $I_k[S]$ 是诚实的,则说明了 S 中的消息攻击者不能够由推导得出,即协议满足秘密性。

(2) 协议认证性分析。

基于理想与诚实理论分析协议认证性思路是:

① 首先构造理想 $I_{K_p}[Mp]$,其中 Mp 是攻击者所掌握的消息,而 K_p 中包含的是攻击者可能知道的密钥。

②生成认证项组成的集合 M_{Auth},并验证条件 $I_{K_p}[Mp] \cap M_{\text{Auth}} = \varnothing$ 是否成立,若成立,则协议满足认证性。

3.3 基于认证测试理论的串空间方法

基于认证测试理论的串空间方法[4,5],是基于串空间模型安全协议形式化分析的最新理论成果。它通过构造认证测试组件,建立安全协议的认证目标,应用认证测试规则判断安全协议是否能够达到其安全目标。目前主要将此理论用于认证协议的认证性分析上,其一般步骤是:

(1)构造测试组件。首先找到认证项新鲜数在串空间的唯一起源点,确定关于新鲜数的测试边,最后确定所构造成的测试组件关于新鲜数构成何种测试。

(2)根据认证测试规则,得到关于认证项新鲜数的转换边。

(3)由(2)的结果,定义认证项中的一个结点,并与串空间中认证项的串相比较,验证是否满足命题要求。

4 串空间形式化方法在协议分析中的应用

下面通过证明 Yahalom 协议,给出串空间形式化方法在安全协议分析中的具体应用。

4.1 Yahalom 协议

Yahalom 协议的目的是第三方服务器 S 为协议主体 A(发起者)、B(响应者) 产生并发送共享会话密钥 K_{AB},并确保 K_{AB} 的机密性,同时 B(响应者) 能有效认证 A(发起者)。该协议参数串的表示如下:

(1) 发起者串 $s \in \text{Init}[A,B,S,N_a,N_b,K]$,在迹映射 tr 下的象为:

$$< + AN_a, - \{BK\ N_aN_b\}K_{as}, + \{ABSN_b\}_K >$$

(2) 响应者串 $s \in \text{Resp}[A,B,S,N,M,K]$,在迹映射 tr 下的象为:

$$< - AN_a, + \{AN_aN_b\}K_{bs}, - \{AK\}K_{bs}, - \{ABSN_b\}_K >$$

(3) 认证服务器串 $s \in \text{Serv}[A,B,N_a,N_b,M,K]$ 在迹映射 tr 下的象为:

$$< - \{AN_aN_b\}K_{bs}, + \{B\,K\,N_aN_b\}K_{as}, + \{AK\}K_{bs} >$$

4.2 秘密性的证明

根据秘密性的含义及基于理想与诚实理论秘密性的证明方法,证明服务器 S 发布的会话密钥 K 是秘密的可转化为证明命题 1 成立。

命题 1　假定 C 是 Yahalom 串空间 $\sum$ 中的一个丛;$A,B \in T_{\text{name}}$;K 是唯一起源的;$K_{AS},K_{BS} \notin K_p$;且 $s_{\text{serv}} \in \text{Serv}[A,B,N_a,N_b,K]$。设 $S = \{K_{AS},K_{BS},K\}$ 且 $K = K/S$,则对每个结点 $m \in C$,$\text{term}(m) \notin I_k[K]$。

证明:

证明一种更强的情形:对每个结点 $m \in C$,$\text{term}(m) \notin I_k[S]$。由于 $S \cap K_p = \varnothing$,$k = k^{-1}$ 且 $K = k \cup S$,由诚实理论可知,仅需证明不存在正常结点 m 是 $I_k[S]$ 的进入点即可。

利用反证法,假定存在一个正常结点 m 是 $I_k[S]$ 的进入点。由此 $\text{term}(m)$ 必然为集合 $I_k[S]$ 的成员。由理想的性质,可知 K_{AS},K_{BS},K 中的某一个是 $\text{term}(m)$ 的子项。由图 1 可见,K_{AS},K_{BS} 并不是任何正常结点的消息项的子项。而 K 起源于服务器 S,故是 $\text{term}(m)$ 的子项。

若 m 为某一个正常串 s 上的一个符号为正的正常结点,则 $K \subset \text{term}(m)$ 意味着:

(1) $s \in \text{Serv}$ 且 $m = < s,2 >$,这里 K 就是 s 的会话密钥;

或者

(2) $s \in \text{Serv}$ 且 $m = < s,3 >$,此时分成两种情形讨论:

情形 1:由于 K 是唯一起源的,故 $s = s_{\text{serv}}$,所以 $\text{term}(m) = \{BKN_aN_b\}_{K_{AS}}$。由理想理论中的第三条性质可得 $K_{BS} \in k$,这与已知矛盾。

情形 2:由于 K 是唯一起源的,故 $s = s_{serv}$,所以 $term(m) = \{AK\}_{K_{BS}}$。由理想理论中的第三条性质可得 $K_{bs} \in k$,这与已知矛盾。

由以上分析,证明开始时假定存在一个正常节点 m 是 $I_k[S]$ 的进入点是错误的,由此结论得到证明。

类似的方法,可以证明由 B 产生的新鲜随机数 N_b,由 A 产生的新鲜随机数 N_a 也是保密的。

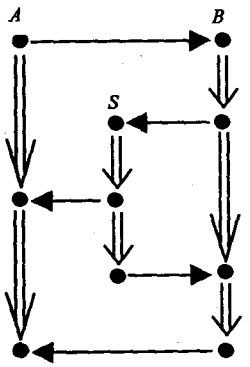

图 1 Yahalo 协议串空间模型图

4.3 认证性的证明

根据认证性的含义及基于认证测试理论认证性的证明方法,证明 B 有效认证 A 和 S 可转化为证明命题 2 成立。

命题 2 假定 C 是 Yahalom 串空间 $\sum$ 中的一个丛;$A \neq B$;在 C 中 N_b 是唯一起源的;且 $K_{AS}, K_{BS} \notin K_p$。若 $s \in Resp[A,B,S,N_a,N_b,K]$ 且 $C - height(s) = 4$,则 C 中必然存在正常串

· $s_{init} \in Init[A,B,S,*,N_b,K]$ 且 $C - height(s_{init}) = 3$

· $s_{serv} \in Serv[A,B,N_a,N_b,K]$ 且 $C - height(s_{serv}) = 3$

证明:

1) 首先应用基于认证测试理论串空间法证明丛 C 中必然存在正常串 $s_{init} \in Init[A,B,S,*,N_b,K]$ 且 $C - height(s_{init}) = 3$。

(1) 构造测试组件。

① 由 Yahalom 改进协议空间模型可知,N_b 唯一起源于 $< s,2 >$,且边 $< s,2 > \Rightarrow^+ < s,4 >$ 是被转换边。因此,边 $< s,2 > \Rightarrow^+ < s,4 >$ 是 N_b 的一个测试。

设 $t_0 = \{ABSN_b\}_K$

② 由 $N_b \subset t_0, t_0$ 是 $< s,4 >$ 的组件且 t_0 不是其它正常结点组件的子项,因此,t_0 是结点 $< s,4 >$ 关于 N_b 的测试组件。

由 ①、② 及 $K \notin K_p$ 得 $< s,2 > \Rightarrow^+ < s,4 >$ 是 t_0 关于 N_b 的输入测试。

(2) 应用认证测试规则。

根据输入测试规则,丛 C 中存在正常结点 m 和 m',使 $m \Rightarrow^+ m'$ 为 N_b 的转换边且 $t_0 \subset term(m')$。

(3) 定义结点 m'。

由(2) 步的分析可得,m' 为某个发起者串中的结点,假设该发起者串为 s'_{init},$s'_{init} = Init[A',B',S,*,N'_b,K']$ 且 $m' = < s'_{init},3 >$,$t_0 \subset term(< s'_{init},3 >)$

(4) 比较串的内容。

通过比较 $term(< s'_{init},3 >)$ 和发起者串中的内容得 $A = A', B = B' N_b = N'_b, K = K'$ 即 $s_{init} = s'_{init}$ 则 $m \Rightarrow^+ m'$ 即 $< s_{init},2 > \Rightarrow < s_{init},3 >$。

故丛 C 中包含发起者串 $s_{init} \in Init[A,B,*,N_b,K]$,并且 $C - height(s_{init}) = 3$。

2) 下面应用认证测试理论证明丛 C 中必然存在正常串 $s_{serv} \in Serv[A,B,N_a,N_b,K]$ 且 $C - height(s_{serv}) = 3$。

(1) 构造测试组件。

① 由 Yahalom 改进协议空间模型可知,N_b 唯一起源于 $< s,2 >$,且边 $< s,2 > \Rightarrow^+ < s,4 >$ 是被转换边。因此,边 $< s,2 > \Rightarrow^+ < s,4 >$ 是 N_b 的一个测试。

设 $t_0 = \{AN_aN_b\}_{K_{BS}}$

② 由 $N_b \subset t_0, t_0$ 是 $< t,2 >$ 的组件且 t_0 不是其它正常结点组件的子项,因此,t_0 是结点 $< t,2 >$ 关于 N_b 的测试组件。

由 ①、② 及 $K_{BS} \notin K_p$ 得 $< s,2 > \Rightarrow^+ < s,4 >$ 是 t_0 关于 N_b 的输出测试。

(2) 应用认证测试规则。

根据输出测试规则,丛 C 中存在正常结点 m 和 m',使 $m \Rightarrow^+ m'$ 为 N_b 的转换边且 $t_0 \subset term(m)$。

(3) 定义结点 m。

由(2) 步的分析可得,结点 m 为负结点,因此 m 为某个服务器串中的结点,假设该服务器串为 s'_{serv},$s'_{serv} = Init[A',B',N'_a,N'_b,K']$ 且 $m = < s'_{serv},1 >$,$t_0 \subset term(< s'_{serv},1 >)$

(4) 比较串的内容。

通过比较 $term(< s'_{serv},1 >)$ 和服务器串中的内容得 $s_{serv} = s'_{serv}$ 则 $m \Rightarrow^+ m'$ 即 $< s_{serv},1 > \Rightarrow < s_{serv},2 >$。

由于服务器串必然会存在一个正结点用于将 K 发送给 B。故丛 C 中包含服务器串 $s_{serv} \in Serv[A,B,N_a,N_b,K]$,并且 $C - height(s_{serv}) = 3$。

5 结 语

文中基于串空间模型内的极小元理论、理想与诚实理论和认证测试理论对安全协议形式化验证方法进行了研究,并将所提出的方法应用于 Yahalom 协议的

(下转第 157 页)

对其仿真数据进行分析而绘制出的平面图。

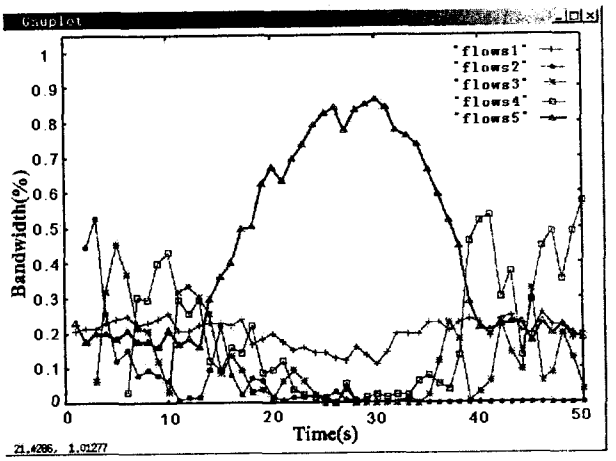

图 3　DDoS 攻击时不采用控制算法

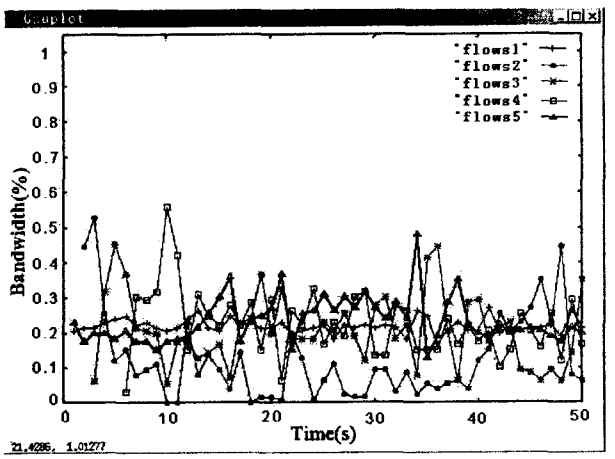

图 4　DDoS 攻击时采用控制算法

对比这两个图,可以明显看出在不使用控制算法的情况下,攻击数据流"flows5"(粗线表示)占用了绝大部分的链路带宽,一部分的正常数据流,比如"flows2"在一段时间内占有的带宽基本为 0;而在使用控制算法的情况下,仿真实验结果明显好转,攻击数据流"flows5"的带宽占有率基本保持在一个稳定的状态下,相应地,正常数据流占有的带宽明显上升。

4　结束语

DDoS 主要是针对 TCP/IP 协议的漏洞进行攻击的,如果能在不改变现有网络体系结构的情况下为这些漏洞"打上补丁"就可以使路由器具有内在的抗 DDoS 攻击的能力。高带宽聚类的控制就是使路由器具有这种能力,当由于 DDoS 攻击而使受害者网络严重拥塞,将 DDoS 攻击流量和正常流量在聚类过程中分开,使攻击流量无法占用正常流量的资源,DDoS 也就无法达到其攻击目的了。

参考文献:

[1] Garher L. Denia－of－Servic Attacks Rip the Internet[J]. Computer,2000, 33(4):12－17.

[2] Lee R B. CE－L 2003－003. Taxonomies of Distributed Denial of Service Networks Attacks, Tools, and Countermeasures[R]. USA:Department of Electrical Engineering, Princeton University, 2003.

[3] Mahajan R, Bellovin S M, Floyd S, et al. Controlling High Bandwidth Aggregates in the Network[J]. ACM SIGCOMM Computer Communication Review,2002,32(3): 62－73.

[4] Hu Yen－Hung,Choi Hongsik,Choi Hyeong－Ah. Packet filtering for congestion control under DoS attacks[C]//Proceedings of the Second IEEE International Information Assurance Workshop (IWIA'04). Washington, DC, USA:[s. n.], 2004:3－18.

[5] Stoica I,Shenker S,Zhang H. Core－stateless fair queueing: a scalable architecture to approximate fair bandwidth allocations in high－speed networks[J]. ACM Transactions on Networking,2003,11(1):33－46.

[6] 徐雷鸣,庞　博,赵　耀. NS 与网络模拟[M]. 北京:人民邮电出版社,2003.

(上接第 154 页)

安全性分析,实验证明这些方法是有效的。

从分析可以得到,基于认证测试理论的串空间方法在分析协议认证性方面比其它两种方法更为简洁、直观,而且这种方法还可查找出协议中存在的漏洞以及存在漏洞的原因;基于理想与诚实理论的串空间方法因理想理论对于刻画消息集合的封闭性有着很好的性质,使得它在分析协议秘密性方面优于其它方法。

参考文献:

[1] Fàbrega F J T,Herzog J C,Guttman J D. Strand Spaces: Why is a Security Protocols Correct[J]. Journal of Computer Security,1999,7(3):191－230.

[2] Ji Q G,Qing S H,Zhou Y B,et al. Study on Strand Space Model Theory[J]. Journal of Computer Science and Technology,2003,18(5):553－570.

[3] Guttman J D,Thayer F J. Key Compromis:Strand Spaces and the Authentication Tests[M]. [s. l.]: Elsevier Science BV, 2002:163－294.

[4] Guttman J D, Fàbrega F J T. Authentication tests and the structure of bundles[J]. Theoretical Computer Science,2002, 283(2):333－380.

[5] Burrows M,Abadi M,Needham R. A logic of Authentication [J]. ACM Transaction in Computer System,1990,8(1):18－36.