基于 Strand 空间的认证协议证明方法研究*

刘东喜, 白英彩

(上海交通大学 计算机科学与工程系,上海 200030)
E-mail: ldx_98@163.net
http://www.sjtu.edu.cn

摘要: Strand 空间是一种新的安全协议分析模型.系统研究了使用 Strand 空间模型证明认证协议存在缺陷的方法.在证明过程中,使用目标细化方法证明了认证属性.通过在该模型中引入消息类型检查机制,简化了证明过程.并将该方法应用到包含三方主体的认证协议.最后得出与相关文献相同的结论.

关 键 词: Strand 空间;认证协议;协议证明;形式化方法
中图法分类号: TP309 文献标识码: A

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.认证协议看似简单,但若确保它正确是极其困难的[1].为此,研究人员采用形式化方法来分析安全协议,这些方法可分为 3 类[2]:推导构造法,利用逻辑推理来分析协议主体的知识和信任的演化情况,比如 BAN 逻辑[3];攻击构造法,利用协议的代数属性建立可能的攻击集合,比如文献[4];证明构造法,证明协议满足其安全性要求,比如文献[5].

在文献[5]中 Thayer,Herzog 和 Guttman 提出了协议的 Strand 空间模型,并证明了 Needham-Schroeder-Lowe 的正确性,但这个协议本身是正确的,而且只包含两个协议主体;在文献[6]中,作者给出了几个有缺陷的协议的 bundle 图,但没有说明如何用 Strand 空间方法去证明这些缺陷的存在.本文以 Woo-Lam 协议为例,给出了使用 Strand 空间模型去证明协议存在缺陷的详细过程,并在 Strand 空间模型中增加了类型检查机制.

本文第 1 节简介 Strand 空间模型.第 2 节介绍认证协议的正确性概念,确定协议证明的目标.第 3 节给出用 Strand 空间模型证明 Woo-Lam 协议的过程.第 4 节总结全文.

1 Strand 空间模型

本节简要描述了文献[5]中提出的 Strand 空间模型中的基本概念.

1.1 项(term)和子项(subterm)

项表示协议消息,A 代表项的集合.项可由原子项经过级连和加密得到,原子项可分为文本项 T 和密钥项 K.

定义 **1**. 符号项是一个有序对$\langle\sigma,t\rangle$,$t\in A$,σ为+或–,记作$+t$ 或$-t$,$+t$ 表示发出项 t;$-t$ 表示接收到项 t.$(\pm A)^*$是符号项的有限序列的集合.

定义 **2**. 项 a 是项 b 的子项,即 $a\sqsubseteq b$,如果下列条件成立:

(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 $a\sqsubseteq g$ 或$\{g\}_k=a$;

(4) $b=g\cdot h$,则要求 $a\sqsubseteq g$ 或 $a\sqsubseteq h$.

* 收稿日期: 2000-10-23; 修改日期:2001-03-01
基金项目: 国家 S219 工程资助项目(2000-A32-09)
作者简介: 刘东喜(1973－),男,山西稷山人,博士生,主要研究领域为安全协议分析,路由器体系结构;白英彩(1936－),男,辽宁沈阳人,教授,博士生导师,主要研究领域为网络技术,分布式系统.

1.2 Strand,Strand空间和Bundle

Strand 是协议角色的一个实例.Strand 空间定义如下:

定义 **3**. 一个 Strand 空间是一个集合Σ,以及映射 $tr:\Sigma\to(\pm A)^*$.

(1) 结点是一个有序对$\langle s,i\rangle$,$s\in\Sigma$,i 满足 $1\le i\le$length($(tr(s))$).结点 $n=\langle s,i\rangle$属于 Strand s,表示为 $n\in s$.结点的集合记为 N.

(2) 如果 $n=\langle s,i\rangle\in N$,那么 index($n$)=$i$,strand($n$)=$s$.如果$(tr(s))_i=\langle\sigma,a\rangle$,那么 term($n$)=+$a$($\sigma$ =+)或 term(n)=–a(σ=–);对于项 a,用 node(+a)或 node(–a)表示它所在的结点.

(3) $n_1,n_2\in N$,那么 $n_1\to n_2$ 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,n_2 属于同一个 s,且 index(n_2)=index(n_1)+1.

(5) 项 t 从结点 n 产生,当且仅当 sign(n)=+;$t\sqsubseteq$term(n);而且对于同一个 Strand 上任何先于 n 的结点 n',$t\not\sqsubseteq$ term(n').

(6) 项 t 从结点 n 惟一产生,当且仅当惟一的结点 n 产生项 t.

所以,Strand 空间构成一个有向图(N,E),N 是结点集合,边 $E=(\to\cup\Rightarrow)$.Bundle 代表协议可能的运行模式,它是有向图(N,E)的子图.

定义 **4**. $C\subseteq E$ 是边的集合,$N_C\subseteq N$ 是由 C 中边相连的结点集合.C 是 Bundle,如果

(1) C 是有限集.

(2) 如果 $n_1\in N_C$,且 sign(n_1)= –,那么有惟一 n_2,满足 $n_2\to n_1\in N_C$.

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

(4) C 是无环的.

因为 Bundle 是一个图,所以在边$\to$和$\Rightarrow$下,结点的关系形成偏序关系,表示为$\le_C$.C 的任何非空结点子集,在$\le_C$ 下都有最小元.

1.3 攻击者模型

攻击者对于通信网络是完全控制的,他的能力可以用一组 Strand P 来表示:

(1) $M[t]$.产生原子文本消息: $\langle+t\rangle$,$t\in T$.

(2) $F[g]$.接收消息: $\langle-g\rangle$.

(3) $T[g]$.接收并多次发送消息: $\langle-g,+g,+g\rangle$.

(4) $C[g,h]$.级连收到的消息: $\langle-g,-h,+g\cdot h\rangle$.

(5) $S[g,h]$.分割收到的消息: $\langle-g\cdot h,+g,+h\rangle$.

(6) $K[k]$.发送密钥: $\langle+k\rangle$,$k\in Key_P$,$Key_P=K_i\cup K_P{}^{-1}\cup K_{px}$.

(7) $E[k,h]$.加密消息: $\langle-h,+\{h\}_k\rangle$,$k\in Key_P$.

(8) $D[k,h]$.解密消息: $\langle-\{h\}_k,+h\rangle$,$k^{-1}\in Key_P$.

其中,Key_p 表示攻击者的密钥集合,包括 i 的公钥 K_i、他的私钥 $K_P{}^{-1}$ 与 x 的共享密钥 K_{px}.

2 正确性概念

认证协议的主要功能是身份认证和密钥分配.在文献[7]中,Woo 和 Lam 把以上两个目标分别转化成对应属性和保密属性.对应属性是说当认证主体以参数 x 完成他的部分协议后,被认证主体也必须以参数 x 参与协议运行,并作为本次运行的发起者,对应属性是保证认证协议的第 1 个目标;保密属性是指消息中的某些字段不能被攻击者访问.

本文中,我们将分别证明协议的对应属性和保密属性.

3 证明 **Woo-Lam** 协议

Woo-Lam 协议是一个使用对称密钥的认证协议,协议规范描述如下:

$A\rightarrow B$:A

$B\rightarrow A$:N_b

$A\rightarrow B$:$\{N_b\}k_{AS}$

$B\rightarrow S$:$\{A,\{N_b\}k_{AS}\}k_{BS}$

$S\rightarrow B$:$\{N_b\}k_{BS}$

协议规范定义了 3 种角色:协议发起者 A,协议响应者 B,以及可信认证服务器 S.它们对应的 Strand 分别为:

(1) 发起者 Strand,对应的消息序列 Init[A,B,N_b]定义为:$\langle+A,-N_b,+\{N_b\}k_{AS}\rangle$;

(2) 响应者 Strand,对应的消息序列 Resp[A,B,N_b]定义为:$\langle-A,+N_b,-\{N_b\}k_{AS},-\{A,\{N_b\}k_{AS}\}k_{BS},-\{N_b\}k_{BS}\rangle$;

(3) 服务器 Strand,对应的消息序列 Serv[A,B,N_b]定义为:$\langle-\{A,\{N_b\}k_{AS}\}k_{BS},+\{N_b\}k_{BS}\rangle$.

3.1 对应属性证明

在 Strand 空间模型中,Woo-Lam 协议的对应属性描述为:假设

(1) Σ是 Woo-Lam 协议的 Strand 空间,C 是含有一个响应者 Strand s 的 bundle,响应者 Strand 对应消息队列 Resp[A,B,N_b];

(2) $k_{AS}\notin Key_P,k_{BS}\notin Key_P$;

(3) N_b 在Σ中从$\langle s,2\rangle$结点惟一产生.

那么,bundle C 中包含一个发起者 Strand t,它的消息队列为 Init[A,B,N_b],其中相同的 N_b 表示初始者和响应者参与同一个消息运行实例,A,B 表示期望的主体身份标识.

用 Strand 证明协议的基本方法是:首先,在 bundle 中根据需要构造一个结点集;其次,考虑结点集的最小元属于哪一种 Strand;最后,对于其余 Strand,分情况判断该最小元是否属于这个 Strand,如果最小元属于该 Strand,说明协议有缺陷.另外,我们引入消息类型检查机制,即协议主体可以判断消息结构,比如消息由哪几个子项级连而成,消息或子项是否经过加密,是否使用期望的加密密钥.

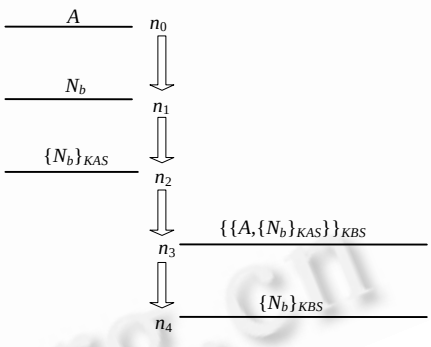

Fig 1 Responder's strand

图 1 响应者 strand

Woo-Lam 协议的对应属性的证明目标可以细分为:首先,存在一个发起者 Strand t,它的消息队列为 Init[x,y,N_b];其次,证明发起者的身份为 A,即 $x=A$;最后,证明与 B 进行身份认证,即 $y=B$.为了证明方便,图 1 给出了响应者 strand 的图形表示.

下面分别证明 3 个目标:

目标 1:存在一个发起者 strand t,它的消息序列为 Init[x,y,N_b].

证明:构造集合 $F=\{n|n\in C\wedge N_b\sqsubseteq\text{term}(n)\wedge N_b\neq\text{term}(n)\}$,可以看出 $n_4\in F$,所以 F 不空,根据 Strand 空间性质,F 必有$\leq_C$最小元,设为 m,sign(m)=+.下面,首先证明 $m\notin p,p\in P$ 和 $m\notin F$.

(1) 证明 $m\notin p,p\in P$.分别讨论 p 的每一个可能的消息序列:

$M[t].tr(p)$的形式为$\langle+t\rangle$,因为 $t\in T$,所以若 $N_b\sqsubseteq t$,那么 $N_b=t$,所以 $m\notin p$.

$F[g].tr(p)$的形式为$\langle-g\rangle$,因为惟一结点的 sign($-g$)=$-$,所以 $m\notin p$.

$T[g].tr(p)$的形式为$\langle-g,+g,+g\rangle$,因为 sign(m)=+,所以若 m=node(+g),那么 node($-g$)$\in F$,这与 m 是最小元矛盾,所以 $m\neq$node(+g),即 $m\notin p$.

$C[g,h].tr(p)$的形式为$\langle-g,-h,+g\cdot h\rangle$,因为合法主体的可接受的消息中没有级连类型,所以排除 $m\in p$.

$S[g,h].tr(p)$的形式为$\langle-g\cdot h,+g,+h\rangle$,由于 g 和 h 的对称性,假设 m=node(+g),那么 node($-g\cdot h$)$\in F$,这与 m 是最小元矛盾,所以 $m\notin p$.

$K[k].tr(p)$的形式为$\langle+k\rangle,k\in Key_P,Key_P=K_i\cup K_P^{-1}\cup K_{px}$,因为 $N_b\notin K_P$,那么 $N_b\not\sqsubseteq k$,所以 $m\notin p$.

$E[k,h].tr(p)$的形式为$\langle-h,+\{h\}_k\rangle,k\in Key_P$,因为对称密钥 $K_{AS}\notin Key_P,K_{BS}\notin Key_P$,所以$\{h\}_k$ 不被合法主体接

受,$m\notin p$.

$D[k,h].tr(p)$的形式为$\langle -\{h\}_k,+h\rangle,k^{-1}\in K_P$,若 $m=\text{node}(+h)$,那么 $N_b\sqsubseteq h$,所以有 $N_b\sqsubseteq\{h\}_k$,且 $N_b\neq\{h\}_k$;这样,$\text{node}(-\{h\}_k)\in F$,这与 m 是最小元矛盾,所以 $m\neq\text{node}(+h)$,即 $m\notin p$. □

(2) 证明 $m\notin S$.

由于服务器 Strand 对应的消息序列 $\text{Serv}[A,B,N_b]$为$\langle -\{A,\{N_b\}K_{AS}\}K_{BS},+\{N_b\}K_{BS}\rangle$,根据 F 的定义可以看出 $\text{node}(-\{A,\{N_b\}K_{AS}\}K_{BS}\in F,+\{N_b\}K_{BS})\in F$.

由于 $\text{node}(-\{A,\{N_b\}K_{AS}\}K_{BS})\Rightarrow+\{N_b\}K_{BS}$,所以 $m\neq\text{node}(+\{N_b\}K_{BS})$;又由于 $\text{sign}(-\{A,\{N_b\}K_{AS}\}K_{BS})=-$,所以 $m\neq\text{node}(-\{A,\{N_b\}K_{AS}\}K_{BS})$,所以 $m\notin S$.

由于 $m\notin p,p\in P$ 和 $m\notin S$,而且 $m\notin\text{Resp}$,所以只有 $m\in\text{Init}$,这就说明存在一个发起者 Strand t,它的消息序列为 $\text{Init}[x,y,N_b]$. □

目标 2:证明发起者的身份为 A,即 $x=A$.

证明: B 是根据协议执行完毕后,根据 N_b 来认证对方是否为 A.构造集合 $G=\{n|\text{term}(n)=\{N_b\}K_{BS}\}$,显然 $n_4\in G$,所以 G 不空,根据 Strand 空间性质,G 必有$\leq_C$最小元,设为 m,$\text{sign}(m)=+$.

由于 K_{BS} 是共享密钥,所以 $m\in\text{Resp}$ 或 $m\in\text{Serv}$.若 $m\in\text{Serv}$,说明被认证主体是 A;若 $m\in\text{Resp}$,说明被认证主体是 B 的另外一个实例.由于不能区分 m 的这两种情况,所以不能证明 $x=A$,只能证明 $x=A$ 或 $x=B$. □

目标 3:证明与 B 进行身份认证,即 $y=B$.

证明:发起者 Strand 的消息序列为$\langle +A,-N_b,+\{N_b\}K_{AS}\rangle$.我们只能通过 N_b 的来源判断认证主体是否为 B,所以构造集合 $H=\{n|\text{term}(n)=N_b\}$,显然$-N_b\in G$,所以 G 不空,根据 Strand 空间性质,G 必有$\leq_C$最小元,设为 m,$\text{sign}(m)=+$.但是由于 N_b 没有加密,所以存在 $m\notin p,p\in P$,不能判断一定 $m\in\text{Resp}$,即不能证明 $y=B$.实际上,这个协议是一个单向认证协议,只要求 B 认证 A,不要求 A 认证 B. □

至此,证明 Woo-Lam 协议的对应属性不能满足,也就是存在协议缺陷,使 B 不可能正确认证 A,这与文献[6]中的结果是一致的.

3.2 保密属性证明

保密性是指协议主体产生的随机数能不能得到保密,Woo-Lam 协议中使用的随机数是 N_b.在本节中,我们从响应者的角度去研究保密性,保密属性在 Strand 空间模型中可以形式化描述为:假设

(1) Σ是 Woo-Lam 协议的 Strand 空间,C 是含有一个响应者 Strand s 的 bundle,响应者 Strand 对应消息队列 $\text{Resp}[A,B,N_b]$;

(2) $K_{AS}\notin Key_P,K_{BS}\notin Key_P$;

(3) N_b 在Σ中从$\langle s,2\rangle$结点惟一产生.

那么,对于$\forall n\in C$,若 $N_b\sqsubseteq\text{term}(n)$,有 n 是以 K_{BS} 或 K_{AS} 为密钥的加密消息,且 $N_b\neq\text{term}(n)$.

证明:从图 1 可以看出,$N_b\sqsubseteq\text{term}(n_1)$,但 n_1 是以明文形式传送,这不满足上述的保密性描述,所以 Woo-Lam 协议的保密属性不满足.这与协议的目的是一致的,Woo-Lam 协议仅是单方认证协议,没有会话密钥分配功能. □

4 结 论

本文使用 Strand 空间模型证明了存在缺陷的 Woo-Lam 协议,得出与相关文献一致的结论.在证明过程中,首先建立协议对应属性和保密属性的 Strand 空间模型,然后构造相应的反映证明属性要求的集合,通过判断该集合最小元的惟一产生结点所在的 Strand 来实现证明目标.在证明过程中,我们在该模型引入类型检查机制,使得证明过程简单化,而且我们把基于 Strand 空间模型的方法用于包含三方主体的认证协议.

References:

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

[2] Gritzalis, S., Spinellis, D., Georgiadis, P. Security protocols over open networks and distributed systems: formal methods for their analysis, design, and verification. Computer Communications, 1999,22(8):695~707.

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

[4] Clarke, E.M., Jha, S., Marrero, W. Using state space exploration and a natural deduction style message derivation engine to verify security protocols. In: Proceedings of the IFIP Working Conference on Programming Concepts and Methods (PROCOMET). New York, 1998. http://www.cs.cmu.edu/~Emarrero/procomet.ps.gz.

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

[6] F'abrega, F.J.T., Herzog, J.C., Guttman, J.D. Strand space pictures. In: Workshop on Formal Methods and Security Protocols. Indianapolis, Indiana, 1998. http://www.cs.bell-labs.com/who/nch/fmsp/8-guttman.ps.

[7] Thomas, Y.C.W., Simon, S.L. A semantic model for authentication protocols. In: Proceedings of the 14th IEEE Symposium on Research in Security and Privacy. Oakland: IEEE Computer Society Press, 1993. 178~194.

Study on the Proof Method of Authentication Protocols Based on Strand Space*

LIU Dong-xi, BAI Ying-cai

(*Department of Computer Science and Engineering, Shanghai Jiaotong University, Shanghai* 200030, *China*)

E-mail: ldx_98@163.net

http://www.sjtu.edu.cn

Abstract: Strand space is a new model for the analysis of security protocols. In this paper, a systematic study is made on how to prove the existence of vulnerabilities in authentication protocols based on the Strand space. During the proof procedure, the authentication property is proved by using the goal-refined method. Moreover, by introducing type-check mechanism into this model, the proof procedure is simplified significantly. In addition, this method is also applied to authentication protocols involved three principals. At last, the same results are got as the relevant literatures.

Key words: Strand space; authentication protocol; protocol proof; formal method

* Received October 23,2000; accepted March 1,2001
Supported by the Foundation of the National S219 Engineering of China under Grant No.2000-A32-09