ISSN 1673-9418 CODEN JKYTA8
Journal of Frontiers of Computer Science and Technology
1673-9418/2008/02(01)-0104-06

E-mail:fcst@public2.bta.net.cn
http://www.ceaj.org
Tel:+86-10-51616056

认证测试方法的改进及应用*

陈力琼[1+],陈 贤[2]
CHEN Liqiong[1+], CHEN Xian[2]

1. 上海交通大学 计算机科学与工程系,上海 200240
2. 西安电子科技大学 通信工程系,西安 710071
1. Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China
2. Department of Communication Engineering, Xidian University, Xi'an 710071, China
+ Corresponding author: E-mail: cxclq2250@126.com

CHEN Liqiong, CHEN Xian. Improvement and application of authentication test. Journal of Frontiers of Computer Science and Technology, 2008,2(1):104-109.

Abstract: Authentication test was proved to be an effective tool of protocol analysis based on strand space. In order to make it to be suitable for analyzing more kinds of protocols and their authentication, security, freshness, non-repudiation and correspondence of principals, authentication test can be improved by making full use of the format of message, fining the procedure of analysis and adding more symbols to represent more goals of security. This improved authentication test combining with model checking automatic tools can solve the problem of space explosion and find detailed attacks as well. It also provides guidance for the design and validation of the protocols.

Key words: strand space; authentication test; correspondence of principals; model checking

摘 要: 基于串空间模型的认证测试方法被证明是一种分析认证协议的有效工具,为了使之适用于类型更多、规模更大的安全协议,并提高其在协议的认证性、可达性、机密性、非否认性、会话密钥的新鲜性及主体间的关联度上的分析能力,对原有的认证测试方法进行改进,充分利用消息格式,细化分析步骤,增添相关符号以分析复杂协议的更多安全特性。利用该方法能缩减模型检测自动化工具的搜索范围,在解决空间爆炸问题的同时有效地找到多方协议的具体攻击路径,而且它对安全协议的设计和验证也具有一定的指导作用。

关键词: 串空间;认证测试;主体关联度;模型检测
文献标识码: A **中图分类号:** TN913

* the National High-Tech Research and Development Plan of China under Grant No.2006AA01Z422 (国家高技术研究发展计划(863)).

Received 2007-07, Accepted 2007-10.

1 前言

随着互联网的迅猛发展,安全协议的分析和设计引起了越来越多的人的关注,随之诞生了很多协议的形式化协议分析理论。目前最流行的协议分析方法分为3类,基于推理结构型方法(如BAN逻辑),基于攻击结构型方法(如模型检测),基于证明结构型方法(如串空间模型[1,2])。与此同时,通用认证协议规范语言CAPSL、中介语言CIL、通信顺序进程CSP及自动化工具SPIN、FDR、athena等的发展都对协议的形式化证明起了推动作用。但目前的各种方法都还存在一定的不足,协议的形式化分析领域尚有很大的发展空间。

串空间理论是建立在Dolev-Yao理论[3]基础上的安全协议分析模型。最小元、理想概念和认证测试[4]方法组成了它的3个核心理论。其中的认证测试方法作为一种形式化分析协议的工具有一些传统方法无法比拟的优点,其分析过程简单,避免了状态爆炸;形式化语言规范化,避免了BAN逻辑由于形式化的不规范引起的问题,也为协议自动化分析工具的设计提供了有力的理论基础。

认证测试方法的出测试、入测试、主动测试能找出很多协议的认证问题。对此方法进一步改进,引入表示签名、MAC等符号的同时,对测试过程的分析进一步完善,使之能够分析多方协议的机密性、新鲜性、不可否认性及主体间的关联度是本文的重点。此外,改进的认证测试方法在设计和验证安全协议上也有重要的应用。

2 更多安全特性的串空间模型描述

2.1 串空间模型

串是协议主体参与的事件序列。诚实主体的串是其收发消息的序列,攻击者的串是其可能收到和发送的所有消息的序列。串空间就是所有串组成的集合,其中包括合法主体的串和攻击者的串。

定义1 丛是串空间的子集,表示一次协议运行的过程。在丛中,结点间形成偏序的关系,表示为$\leq_C$,C的任何非空结点子集都有$\leq_C$最小元。

定义2 串空间s由集合Σ以及轨迹影射$\mathrm{tr}:\Sigma\rightarrow(\pm A)^*$组成,其特性如下:

(1)结点n是个二元组$<s,i>$,其中$s\in\Sigma$,i为满足$1\leqslant i\leqslant length(\mathrm{tr}(s))$的整数。$n\in s$,结点集合为$N$,显然每个结点都属于唯一的串。

(2)若$n=<s,i>\in N$,则$index(n)=i$,$strand(n)=s$。定义$term(n)=(\mathrm{tr}(s))_i$,即$term(n)$是$\mathrm{tr}(s)$中的第$i$个符号项,$sign(n)=+$表示$n$为正结点,$sign(n)=-$表示$n$为负结点;$uns_term(n)=((\mathrm{tr}(s))_i)_2$为$s$中第$i$个符号项的无符号部分。

(3)若$n1,n2\in N$,$n1\rightarrow n2$表示$n1$向$n2$发送一条消息a,并且$term(n1)=+a$,$term(n2)=-a$。

(4)若$n1,n2\in N$,$n1\Rightarrow n2$表示$n1$、$n2$是同一串上的结点,并且$index(n1)=index(n2)-1$。串空间通过边$\rightarrow$,$\Rightarrow$表示结点间的偏序关系。

(5)一个无符号项t出现在结点$n\in N$中,当且仅当$t\sqsubset term(n)$。

(6)无符号项t由结点$n\in N$产生,当且仅当$sign(n)=+$,$t\sqsubset term(n)$,并且对于任何一个先于n出现的结点n',都有$t\not\sqsubset term(n)$。

(7)无符号项t是唯一起源的,当且仅当t产生于唯一的结点$n\in N$。

由此可见,串空间组成了一个有向图$G=(N,E)$,N是串中结点的集合,$E=(\rightarrow,\Rightarrow)$是边的集合。

定义3 设C为边的集合,N为C中边所连接的结点集合,若C满足以下条件,则称C为丛:

(1)C是有限的。

(2)如果$n1\in N$,并且$sign(n1)=-$,则存在一个唯一的结点$n2$,$n2\rightarrow n1\in C$。

(3)如果$n1\in N$,并有$n2\Rightarrow n1$,则$n2\Rightarrow n1\in C$。

(4)C是非循环的。

2.2 安全特性在串空间中的描述

能用串空间模型的术语对更多的安全特性进行如下描述:

(1)认证性与可达性

如果满足特定数据项的起源假设,且串 S 在丛 C 中的长度为 i,则要求串 S_0 在丛 C 中的长度为 j,且 S_0 在规定的数据集上和 S 达成共识,这样就称串 S 的主体对串 S_0 的主体进行了认证,且 j 的数值大小能够表示协议最终的可达性。

(2)机密性

如果满足特定数据项的起源假设,且串 S 在丛 C 中的长度为 i,则要求丛 C 中没有一个结点 n 满足 $term(n)=t$,其中机密数据被包含在 t 中且能被攻击者通过某种途径获取。

(3)新鲜性

假设数据项被认为是新鲜的时限大于合法主体串中任意两个结点的时间间隔,那么如果丛 C 中存在一个诚实结点 n 及串 $m_0 \Rightarrow^{+} m_1$,且 $m_0 \leq_C n \leq_C m_1$,则 m_1 认为 n 为本轮结点,唯一起源于 n 结点的数据项被 m_1 认为是 1 度新鲜的。同理若另一结点 r 被 n 认为是本轮结点,则 r 也被 m_1 认为是本轮结点,唯一起源于 r 的数据项被 m_1 认为是 2 度新鲜的。如此类推,指定被认为是 i 度新鲜的数据项能够满足新鲜性要求,其中 $i \leqslant N$,常数 N 由具体协议决定。

(4)非否认性

若属于丛 C 的串 S 中存在结点 n,$term(n)=-[..N..]_K$ 或 $H_K(..N..)$,其中 $[\ ]_K$ 和 $H_K(\ )$ 分别表示用私钥 K 签名或哈希后的数据,则能证明丛 C 包含另一串 S_0,$term(<S_0,j>)=+[..N..]_K$ 或 $h_K(..N..)$。也就是说串 S 的主体可以提供证据证明串 S_0 在丛 C 中的长度至少为 j。

下文中若称密钥 K 是安全的,则表明 K 不能有攻击者通过各种途径获得。

3 认证测试方法的改进

3.1 改进的原理

3.1.1 出测试

(1)原始的出测试

如图 1 所示,$m_0 \Rightarrow^{+} m_1$ 属于丛 C,数据项 a 是唯一起源的,且只以 $\{...a...\}_K$ 的形式被结点 m_0 发送出去,其中 K 是安全的,而后 a 又以 $\{...a...\}_K$ 外的其它形式由结点 m_1 接收,则丛 C 中一定还存在另一合法主体的边 $n_0 \Rightarrow^{+} n_1$,其中,$term(n_0)$ 包含分量 $\{...a...\}_K$,而 $term(n_1)$ 包含分量 t',$a \subset t'$,$t' \neq \{...a...\}_K$。把 $n_0 \Rightarrow^{+} n_1$ 称为变换边,符号表示成 $\{...a...\}_K \rightarrow a$,且 $m_0 \leqslant n_0 \leqslant n_1 \leqslant m_1$。

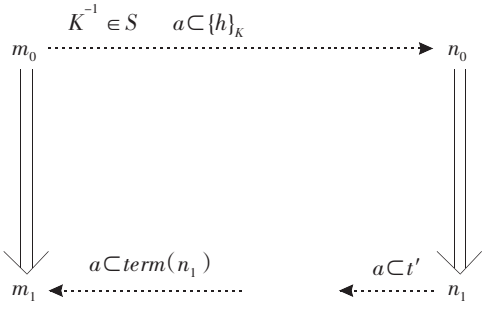

图 1 原始出测试

Fig.1 Original outgoing test

(2)改进的出测试

在原始出测试的基础上,若 $t'=\{...a...\}_{k'}$,$k' \neq k$ 且 k' 是安全的,则要么(1)$t' \subset term(m_1)$,要么(2)$t' \not\subset term(m_1)$。若满足(2)的条件,推断得必存在另一合法主体接收分量 t',且此后发送分量 t'',$a \subset t''$,$t' \neq t''$。再对 t'' 像对 t' 那样分析,直到满足(1)的条件为止。

由拓展的出测试得到,对一轮出测试而言,可能存在多条变换边,也就是 m_0、m_1 的主体对多个合法主体进行了认证。

3.1.2 入测试

(1)原始的入测试

如图2所示,$m_0 \Rightarrow^{+} m_1$属于丛C，若数据项a以$\{...a...\}_K$的形式被结点m_1接收,K是安全的,且a此前以不同于$\{...a...\}_K$的形式被结点m_0发送,则丛C中一定还存在另一合法主体的边$n_0 \Rightarrow^{+} n_1$，其中$\{...a...\}_K \subset term(n_1)$,$\{...a...\}_K \not\subset term(n_0)$。令分量$t \subset term(n_0)$,$a \subset t$,把$n_0 \Rightarrow^{+} n_1$称为变换边,符号表示为$a \rightarrow \{...a...\}_K$,且$m_0 \leqslant n_0 \leqslant n_1 \leqslant m_1$。

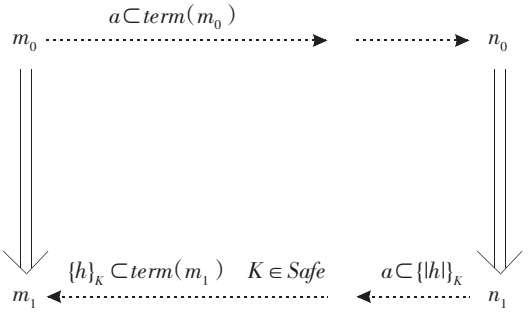

图2 原始入测试

Fig.2 Original incoming test

(2)改进的入测试

在原始入测试的基础上,如果$t \not\subset term(m_0)$,且$t=\{...a...\}_{k'}$,$k' \neq k$,k'是安全的,则丛C中一定还存在另一合法主体在结点n_0前发送分量t,同时该主体此前必然收到分量t',其中$a \subset t'$,$t \neq t'$。再对t'像对t那样分析,直到它是$term(m_0)$的分量为止。

由拓展的入测试得到,对一轮入测试,可能存在多条变换边,则m_0、m_1的主体对多个合法主体进行了认证。

3.1.3 主动测试

丛C的一个结点n,$\{h\}_K \subset term(n)$,且K是安全的,则丛C中必存在另一个合法结点m,使得$\{h\}_K \subset term(m)$。

以上就是三种认证测试方法的基本原理及其拓展。拓展后的认证测试方法能够有效地分析三方甚至多方参与的安全协议,据此来设计多方协议,也是对原始认证测试方法进行拓展的重要价值所在。

3.2 改进后的能力分析

拓展的认证测试方法可以对协议的认证性、机密性、非否认性、数据项的新鲜性及主体间的关联度等进行分析。

(1)认证性

合法主体通过一轮测试能得知哪些串的主体参与了协议的执行,对安全密钥加密的测试分量进一步分析能使合法主体在参与者身份、随机数、会话密钥等信息上达成共识。

(2)机密性

若数据项a在一轮测试中一直被包含在安全密钥加密的分量中，则在本轮测试期间,a的机密性得到了保证。

(3)新鲜性

若合法主体通过一轮测试得到丛C的多个结点满足$m_0 \leqslant .. \leqslant n_0 \leqslant n_1 \leqslant .. \leqslant m_1$，且数据项$a$唯一起源于某一中间结点,则$a$对结点$m_1$是新鲜的。多轮测试能得到数据项的多度新鲜性。

(4)非否认性

若一轮测试中，结点m_1接收了被某个合法主体的私钥签名或哈希的数据项，则m_1的主体就可以把它作为证据来向第三方证明私钥的拥有者确实参加了本次协议的执行。

(5)关联度及可达性

通过多轮测试,还能得到所有合法主体间的关联度。关联度$Correspondence_{AB}$定义如下:若主体A在一轮测试后对B的身份及其他数据项进行了认证,即认为存在主体B的变换边$n_0 \Rightarrow^{+} n_1$，则$Correspondence_{AB}=index(n_1)>Correspondence_{AB}?index(n_1):Correspondence_{AB}$，而$Correspondence_{AA}$为主体$A$的串长度。每个合法主体在多轮测试后,能得到主体间关联度矩阵,矩阵中的每个元素a_{ij}表示主体i在协议执行

完后认为主体 j 参加了几次消息的接收或发送。关联度矩阵能有效地表示协议的可达性。

4 实例分析

下面以 Yahalom 协议为例,运用拓展的认证测试方法分析其多种安全特性。

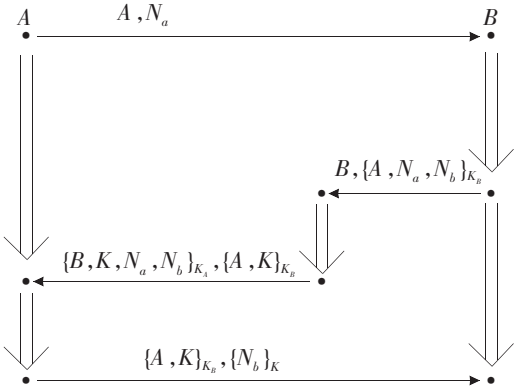

图 3 Yahalom 协议的串空间模型

Fig.3 Strand space of Yahalom protocol

对主体 B 进行认证分析,假设存在丛 C 的串 $Sr\in Resp[A,B,N_a,N_b,K]$,$N_b$ 是唯一起源的,由于 K_B 是安全的,则<Sr,2>⇒<Sr,3>是对分量$\{A,N_a,N_b\}_{k_B}$的改进出测试,则丛 C 中必存在变换边$\{A,N_a,N_b\}_{k_B}\rightarrow N_b$,通过对主体串格式的分析,此变换边只可能包含在串 $Ss\in Serv[A,B,N_a,N_b,K']$中。假设 K'唯一起源于丛 C 的某一结点 n,$n\leq_C$<Sr,3>且 K'是安全的,既然 $K'\not\subset\{A,N_a,N_b\}_{k_B}$,则 K'不一定就是 K。

由出测试的拓展部分得到,N_b 以$\{B,K',N_a,N_b\}_{K_A}$的形式再次由<Ss,2>发送出去,且 K_A 是安全的,则此分量必定被另一合法主体接收,根据合法主体的串格式得到,此结点就是<Si,2>,其中 $Si\in Init[A,B,N_a,N_b,K']$,因此 $term(<Si,3>)$包含$\{N_b\}_{K'}$,此后分量$\{N_b\}_{K'}$必定被另一个合法主体接收,若接收结点为<Sr',3>,$Sr'\in Resp[**,N_b,K']$,由 N_b 的唯一起源性得到 $Sr'=Sr,K'=K$。

主体 B 通过一轮拓展的出测试得到丛 C 中存在 $Ss\in Serv[A,B,N_a,N_b,K]$,$Si\in Init[A,B,N_a,N_b,K]$,即 B 在执行完一次协议后对协议发起方 A 和服务器 S 进行了认证。

另外,通过本轮测试还能保证会话密钥对于主体 B 的新鲜性,K 唯一起源于本轮测试的中间结点,因此它对<Sr,3>来说是新鲜的。N_b 在本轮测试中一直包含在安全密钥加密的分量中,所以对主体 B 而言,N_b 的机密性得到了保证。因为 B 没有得到用 A 或 S 的私钥签名或哈希的分量,所以协议的非否认性不能得到保证。

同理对主体 A 进行认证分析,假设丛 C 的串 $Si\in Init[A,B,N_a,N_b,K]$,通过改进入测试,$A$ 只能肯定存在丛 C 的串 $Ss\in Serv\ [A,B,N_a,N_b,K]$,$Sr\in Resp[A,B',N_a,N_b,K']$,因此主体 A 不能完成对主体 B 的认证。

在所有轮测试后得到主体间关联度矩阵:

$$Correspondence(A,B,S)=\begin{bmatrix}3&0&2\\3&3&2\\0&2&0\end{bmatrix}$$

5 结论及进一步应用

以上对改进的认证测试方法的原理和应用作了详细的阐述,并证明改进后的认证测试方法除具备原始认证测试方法的优势外,还能对各种规模的安全协议的认证性、机密性、不可否认性及数据项的新鲜性等特性进行有效的分析,得到的主体间关联度矩阵也为协议的进一步分析和自动验证程序的开发提供了依据。

改进的认证测试方法虽然有很强的分析能力,但也有其不足之处,即它不能找出攻击者的具体攻击路径。把它和模型检测的方法相结合,先利用拓展的认证测试方法找出协议不满足安全特性的原因,然后分析有可能造成这些原因的状态,用模型检测的自动化

工具(如 FDR)只对这些不安全状态进行搜索以寻找具体攻击路径，这就大大缩小了搜索的空间范围,解决模型检测方法的空间爆炸问题的同时也找到了具体攻击路径。

改进的认证测试方法在协议的设计和验证上也有重要的应用。根据协议所要求的安全特性,在用串空间建模时设计各个合法主体的多轮测试并构造相关的测试分量，即把安全特性所涉及的相关数据项(如协议主体标识、会话密钥、签名等)加入测试分量中,保证每个合法主体能通过几轮测试最终达到协议的安全目标。最后利用改进的认证测试方法对设计的安全协议进行验证,完善协议的不足之处,这种方法在保证协议正确性的同时又大大简化了设计的步骤。

今后希望能对改进的认证测试方法进一步完善，使它能够分析更多的安全特性和更多的安全协议。改进的认证测试方法的自动化也是需要解决的问题。

References:

[1] Fàbrega F J T, Herzog J C, Guttman J D. Strand spaces: why is a security protocol correct?[C]//Proc of the 1998 IEEE Symp on Security and Privacy. Los Alamitos:IEEE Computer Society Press, 1998:160-171.

[2] Fàbrega F J T, Herzog J C, Guttman J D. Strand spaces: proving security protocols correct[J]. Journal of Computer Security, 1999,7(2/3):191-230.

[3] Dolev D, Yao A. On the security of public key protocol[J]. IEEE Transactions on Information Theory, 1983,29(2): 198-208.

[4] Guttman J D, Thayer F J. Key compromise, strand spaces and the authentication tests[M]. [S.l.]: Elsevier Science BV, 2002.

陈力琼(1982-),女,浙江温州人,硕士研究生,2001 年于西安电子科技大学获软件工程学士学位,目前是上海交通大学计算机系统与结构专业硕士生,研究方向:密码学、密码协议。

CHEN Liqiong was born in 1982. She received her B.S. degree in Software Engineering from Xidian University in 2001, and now is a master in Computer Science at Shanghai Jiao Tong University. Her research interests include cryptography and protocol analysis.

陈贤(1983-),男,浙江温州人,硕士研究生,2001 年于西安电子科技大学获通信工程学士学位,目前是西安电子科技大学通信工程专业硕士生,研究方向:协议分析、J2EE、数字信号处理等。

CHEN Xian was born in 1983. He received his B.S. degree in Communication Engineering from Xidian University in 2001, and now is a master in Communication Engineering at Xidian University. His research interests include protocol analysis, J2EE and DSP.