文章编号:1671 - 6833(2010)03 - 0050 - 04

认证测试方法的扩展及其应用

周清雷, 毋晓英

(郑州大学 信息工程学院,河南 郑州 450001)

摘 要: 基于串空间模型的认证测试方法分析协议的安全性有一定的局限性,只能分析有限的协议. 因此,对基于串空间模型的认证测试方法进行了扩展,通过修改测试分量和认证测试规则,对该方法进行了改进,运用扩展后的认证测试方法对使用签名和哈希函数的 TLS 协议进行了分析,扩大了认证测试方法的使用范围;并提出了对测试分量新鲜性的检验,进一步完善了认证测试方法.

关键词: 串空间模型;认证测试;TLS 协议; 哈希函数;测试分量

中图分类号: TP309 **文献标识码**: A

0 引言

安全协议的形式化分析主要有基于推理的结构性方法、基于攻击的结构性方法和基于证明的结构性方法. 串空间模型是基于证明结构性方法的典型代表,它把安全协议的形式化分析推到了一个新的高度.

Guttman 提出的认证测试方法,是串空间理论发展过程中的一个重要事件. 认证测试方法通过构造测试分量对协议进行分析,使协议的分析过程更加简洁和直观,但它的分析范围有一定的局限性,不能分析使用签名和哈希函数的协议.

笔者首先介绍串空间的基础知识,然后给出扩展后的认证测试方法,并用该方法对使用签名和哈希函数的 TLS 协议进行分析,说明扩展后方法的有效性.

1 串空间理论

本节主要介绍这种基于代数系统的串空间模型,包括串空间模型的基本概念与构想,基本假设以及构造串空间的方法.

定义 1.1 符号项是一个二元组 $< \delta, a >$,其中 $a \in A$ 且 $\sigma = \{+, -\}$,记符号项为 $+t$ 或 $-t$. $(\pm A)^*$ 是符号项的有限序列集合,记 $(\pm A)^*$ 中的元素为 $< < \sigma_1, a_1 >, \cdots, < \sigma_n, a_n > >$.

在安全协议中,主体可以接收项,也可以发送项. 在串空间模型中,用加号表示发送项,减号表示接收项.

定义 1.2 A 上的串空间为一个集合 $\sum$ 以及它的迹映射 $\mathrm{tr}: \sum \to (\pm A)^*$.

定义 1.3 构造串空间的方法:

(1) 节点是二元组 $< s, i >$,其中 $s \in \sum$ 且 i 为满足 $1 \leqslant i \leqslant \mathrm{length}(\mathrm{tr}(s))$ 的整数. 结点集合记为 N,称结点 $< s, i >$ 属于串 s. 显然,每一个结点属于唯一的一个串.

(2) 若 $n = < s, i > \in N$,则 $\mathrm{index}(n) = i$,且 $\mathrm{strand}(n) = s$. 定义 $\mathrm{term}(n)$ 为 $(\mathrm{tr}(s))_i$,即串 s 的迹中的第 i 个符号项. 定义 $\mathrm{unsterm}(n) = ((\mathrm{tr}(s))_i)_2$,即串 s 的迹中的第 i 个符号项的无符号部分.

(3) 存在一个边 $n_1 \to n_2$,当且仅当存在某一个 $a \in A$,使得 $\mathrm{term}(n_1) = +a$ 且 $\mathrm{term}(n_2) = -a$. 因此,这类边表示结点 n_1 发送消息 a,结点 n_2 接收消息 a,记录了串间的一种因果连接.

(4) 若 $n_1 = < s, i > \in N$,且 $n_2 = < s, i+1 > \in N$,则存在边 $n_1 \Rightarrow n_2$. 这类边表示 n_1 是 n_2 在串 s 上的直接因果前驱. 用 $n' \Rightarrow n$ 表示 n' 是 n 在同一个串 s 上的因果前驱(不一定是直接因果前驱).

(5) 一个无符号项 t 出现在 $n \in N$,当且仅当 $t \subset \mathrm{term}(n)$.

(6) 令 I 为无符号项集合. 称结点 $n \in N$ 是 I

收稿日期:2009 - 12 - 18;修订日期:2010 - 03 - 03

基金项目:国家"863"计划资助项目(2007AA010408)

作者简介:周清雷(1962 -),男,河南辉县人,郑州大学教授,CCF 高级会员,博士生导师,主要研究方向为安全协议分析、模型检测、自动机.

的入口点,当且仅当term(n) = $+t$,其中$t \in I$,且对所有的结点$n' \Rightarrow^{+} n$,term(n') $\notin I$.

(7) 无符号项t起源于结点$n \in N$,当且仅当n是集合$I = \{t': t \subset t'\}$的入口点.

(8) 无符号项t是唯一起源的,当且仅当t起源于唯一的一个结点$n \in N$.集合N以及两类边$n_1 \rightarrow n_2$和$n_1 \Rightarrow n_2$的集合构成一个有向图$< N, (\rightarrow, \Rightarrow) >$.

定义1.4　从[3]是串空间中一个重要的概念,具体定义如下:

假设$\rightarrow_C \subset \rightarrow$;$\Rightarrow_C \subset \Rightarrow$;且$C = < N_C, (\rightarrow_C \cup \Rightarrow_C) >$是$< N, (\rightarrow \cup \Rightarrow) >$的一个子图,$C$是丛当且仅当

(1)C是有限的无环图;

(2) 若$n_2 \in N_C$,且term(n_2)为负,则存在唯一的结点n_1,使得$n_1 \rightarrow_C n_2$;

(3) 若$n_2 \in N_C$,且$n_1 \Rightarrow n_2$,则$n_1 \Rightarrow_C n_2$.

设C为丛,定义s串的C高度,记为C—hight(s),是满足$< s, i > \in C$的最大的i值.s在C中的迹为C—trace(s) = $< (\mathrm{tr}(s))_1, \ldots, (\mathrm{tr}(s))_m >$,其中$m = C$—hight($s$).

命题1.1 项与二元算子

$T \subseteq A$是正文集合,表示原子消息.

$K \subseteq A$是密钥集合,其中K与T是不相交集.K中有一个一元算子inv:$K \rightarrow K$.假定inv是单射的,它将非对称密码系统中的密钥对中的一个映射为另一个;将对称密钥映射为自身.

扩展后的二元算子如下.

encr:$K \times A \rightarrow A$,

join :$A \times A \rightarrow A$,

sign:$K \times A \rightarrow A$,

hash:$A \times K \rightarrow K$.

应用串空间模型证明安全协议的正确性时,需要用到自由加密假设.自由假设规定,一个密文只能以一种方式看待.然而用串空间模型来分析使用签名的协议时,需要用到自由签名假设,一个签名也只能以一种方式看待,下面给出扩展后的自由假设:

命题1.2　对于$m, m' \in A$,且$K, K' \in K$,

(1) $\{m\}_K = \{m'\}_{K'} \Rightarrow m = m' \wedge K = K'$

(2) $[m]_K = [m']_{K'} \Rightarrow m = m' \wedge K = K'$

串是协议执行的事件序列,串空间模型既有合法主体的串也有攻击者[4]串.其中攻击者所具有的原子行为是通过攻击者迹来描述的,它总结了攻击者丢弃消息、生成消息、连接消息,以及攻击者应用他所知道的密钥进行密码运算的能力,下面给出扩展后的攻击者原子行为

定义1.5　攻击者迹包括的内容

(1) M. 正文消息:$< +t >$,其中$t \in T$;

(2) K. 密钥:$< +K >$,其中$K \in K_P$;

(3) C. 连接:$< -g, -h, +gh >$;

(4) S. 分解:$< -gh, +g, +h >$;

(5) E. 加密:$< -K, -h, +\{h\}_K >$;

(6) D. 解密:$< -K^{-1}, -\{h\}_K, +h >$;

(7) S_g. 签名:$< -K, -h, +[h]_K >$;

(8) H. 哈希运算:$< -g, +\mathrm{hash}(g) >$.

2　认证测试方法的扩展

认证测试方法是通过构造测试分量,应用认证测试规则来分析安全协议是否能达到其预期的安全目标,但原有的认证测试方法[5]受测试分量的限制,使它的分析范围有一定的局限性,不能用来分析使用签名和哈希函数的协议,本节将给出扩展后的认证测试方法的主要概念及其规则.

定义2.1　项

称项t_0为项t的分量,若$t_0 \subset t, t_0$不是级联项,且任何满足$t_0 \subset t_1 \subset t$的$t_1 \neq t_0$是级联项.那么,分量可能是原子值,加密项或签名项.称项t在结点$n = < s, i >$是新项,如果t是项term(n)的分量,但t不是结点$< s, j >$的分量,其中$j < i$.

定义2.2　称边$n_1 \Rightarrow^{+} n_2$是对于$a \in A$的被变换边(变换边),如果n_1为正(负)且n_2为负(正),$a \subset \mathrm{term}(n_1)$,且存在一个$n_2$的新分量$t_2$,使得$a \subset t_2$.

定义2.3　称边$n_0 \Rightarrow^{+} n_1$是对于a的测试,如果a唯一地产生在n_0,且$n_0 \Rightarrow^{+} n_1$是对于a的被变换边.

定义2.4　测试分量

在串空间$\sum$下,称正则串的某个部分为测试,它的存在将保证其他正则串在丛中的存在.称项$t = [h]_K$或$t = \{h\}_K$是项a在结点n中的测试分量,如果

(1) $a \subset t$且t是n的分量;

(2) t不是任何正则结点$n' \in \sum$的分量的真子项.

命题2.1　三种认证测试方法

(1) 出测试:称边$n_0 \Rightarrow^{+} n_1$是a在$t = [h]_K$或$t = \{h\}_K$中的出测试,如果它是对于a的测试,且$K^{-1} \notin K_P$,这里K_P表示不安全密钥集合.除t外a不在n_0的任何分量中出现,且t是a在n_0中的测试分量.

(2) 入测试:称边 $n_0 \Rightarrow^+ n_1$ 是 a 在 $t_1 = [h]_K$ 或 $t_1 = \{h\}_K$ 中的入测试,如果它是对于 a 的测试,且 $K \notin K_P$. 并且 t_1 是对于 a 在 n_1 中的测试分量.

(3) 主动测试:称负结点 n 是对于 $t = [h]_K$ 或 $t = \{h\}_K$ 的主动测试,如果 t 是对于 n 中任何 a 的测试分量,且 $K \notin K_P$.

扩展后的认证测试规则如下:

命题 2.2 认证测试规则

2.2.1 出测试原理:

令 C 为丛,$n' \in C, n \Rightarrow^+ n'$ 是 a 在 t 中的出测试. 那么:

(1) 存在正则结点 $m, m' \in C$,使得 t 是 m 的分量,且 $m \Rightarrow^+ m'$ 是对于 a 的变换边;

(2) 假设除此之外 a 只在 m' 的分量 $t = [h_1]_{K_1}$ 或 $t_1 = \{h_1\}_{K_1}$ 中出现,且 t_1 不是任何正则分量的真子项,并且 $K_1^{-1} \notin K_P$. 于是,存在一个负正则结点 m'',其中 t_1 是 m'' 的分量.

2.2.2 入测试原理:

令 C 为丛,$n' \in C$;令 $n \Rightarrow^+ n'$ 是 a 在 t' 中的入测试. 那么,存在正则结点 $m, m' \in C$,使得 t' 是 m' 的分量,且 $m \Rightarrow^+ m'$ 是对于 a 的变换边.

2.2.3 主动测试原理:

令 C 为丛,$n \in C$,n 是对于 $t = [h]_K$ 或 $t = \{h\}_K$ 的主动测试. 那么,存在一个正正则结点 $m \in C$,使得 t 是 m 的分量.

由于主动测试是建立在测试分量满足新鲜性的假设基础上,因此用主动测试分析的协议需要附加对其测试分量新鲜性的验证,这也是对主动测试原理的补充.

3 实例应用

本节通过对 TLS 协议进行分析,说明扩展后的认证测试方法在安全协议分析中的应用.

3.1 简化版的 TLS 协议

(1) $C \rightarrow S$:C

(2) $S \rightarrow C$:$S[\,|g^x|\,]_{K_S}$

(3) $C \rightarrow S$:$[\,|g^y|\,]_{K_C}\{\,|T_1CS|\,\}_{K'}$

(4) $S \rightarrow C$:$\{\,|T_2CS|\,\}_{K'}$

其中,g 是一个循环群生成元;x, y 是从 $\{1, 2 \ldots |G|\}$ 随机选择的,签名过程的唯一性取决于选择的随机数;T_1, T_2 是不同的标签;K' 是对称密钥,通过 $\mathrm{hash}(g^{xy})$ 而得.

3.2 TLS 协议的串空间模型

其中:$M_1 = C$;$M_2 = S[\,|g^x|\,]_{K_S}$;$M_3 = [\,|g^y|\,]_{K_C}\{\,|T_1CS|\,\}_{K'}$;$M_4 = \{\,|T_2CS|\,\}_{K'}$ 协议中发起者 C 和响应者 S 对应的串分别为:

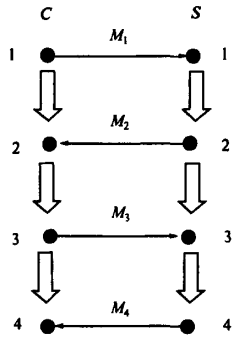

图 1 TLS 协议串空间模型

Fig.1 Strand space model of TLS protocol

(1) 发起者串 $\mathrm{Init}[C, S, g^x, g^y] = \langle +C, -S[\,|g^x|\,]_{K_S}, +[\,|g^y|\,]_{K_C}\{\,|T_1CS|\,\}_{K'}, -\{\,|T_2CS|\,\}_{K'} \rangle$

(2) 响应者串 $\mathrm{Resp}[C, S, g^x, g^y] = \langle -C, +S[\,|g^x|\,]_{K_S}, -[\,|g^y|\,]_{K_C}\{\,|T_1CS|\,\}_{K'}, +\{\,|T_2CS|\,\}_{K'} \rangle$

3.3 TLS 协议认证性分析

前提假设 C_1 为 $\sum$ 中的丛,$K_C, K_S, K' \notin K_P$,$g^x \neq g^y$,且 g^y 是由发起者串 S_i 唯一产生的,g^x 是由响应者串 S_r 唯一产生的.

3.3.1 发起者对响应者的认证

(1) 构造测试分量:发起者串 $S_i = \mathrm{Init}[C, S, g^x, g^y]$,据认证测试的定义,发起者串 S_i 中不存在出测试和入测试的被转换边,因此认证测试的出测试和入测试原理不能使用. 可以用主动测试进行分析,$t = S[\,|g^x|\,]_{K_S}$ 是 g^x 在 $\langle S_i, 2 \rangle$ 结点 $S[\,|g^x|\,]_{K_S}$ 的主动测试.

(2) 运用测试规则:根据主动测试原理,可得存在一个正正则结点 $m \in C_1$ 且 t 是 m 的分量,假设 m 是串 $S_1 = [C', S', g^{x'}, g^{y'}]$ 中的结点.

(3) 项的匹配:由于 g^X 唯一起源于响应者串,则 $S_r = S_1$,根据响应者串 $S_r = \mathrm{Resp}[C, S, g^x, g^y]$ 中项的匹配关系,可得 $\langle S_r, 2 \rangle$ 即为 m 所对应的结点,比较两串的内容可得到:$S = S', g^x = g^{x'}, C = C', g^y = g^{y'}$.

(4) 测试分量新鲜性验证:测试分量 $t = S[\,|g^x|\,]_{K_S}$ 中包含接收者能识别的新鲜因子,综合第(3)步结果可得,发起者能够成功地认证响应者.

3.3.2 响应者对发起者的认证

(1) 构造测试分量:响应者串 $S_r = \mathrm{Resp}[C, S, g^x, g^y]$,其中也不存在出测试和入测试分量.

同上运用主动测试,$t' = [\,|g^y|\,]_{Kc}$ 是 g^y 在 $< S_r,3 >$ 结点 $[\,|g^y|\,]_{Kc}\{\,|T_1CS|\,\}_{K'}$ 的主动测试.

(2) 运用测试规则:根据主动测试原理,可得存在一个正则结点 $m' \in C_1$ 且 t' 是 m' 的分量,假设 m' 是串 $S_2 = [C'',S'',g^{x''},g^{y'}]$ 中的结点.

(3) 项的匹配:由于 g^y 唯一起源于发起者串,则 $S_i = S_2$,根据发起者串 $S_i = \mathrm{Init}[C,S,g^x,g^y]$ 中项的匹配关系,可得 $< S_i,3 >$ 即为 m' 所对应的结点,比较两串的内容可得到:$C = C'',g^y = g^{y'},S = S'',g^x = g^{x''}$.

(4) 测试分量新鲜性验证:测试分量 $t' = [\,|g^y|\,]_{Kc}$ 中没有接收者可识别的新鲜因子,虽然第(3)步响应者能够对发起者标识符和随机数进行验证,但测试分量不满足新鲜性条件,因此响应者对发起者的认证失败.

用扩展后的认证测试方法发现了TLS协议存在针对消息新鲜性重放攻击的缺陷,文献[6]中指出了针对此缺陷的攻击,并给出TLS协议的改进版本:

(1) $C \rightarrow S : C$

(2) $S \rightarrow C : S[\,|g^x|\,]_{K_s}$

(3) $C \rightarrow S : [\,|C,g^x,g^y|\,]_{Kc}\{\,|T_1CS|\,\}_{K'}$

(4) $S \rightarrow C : \{\,|T_2CS|\,\}_{K'}$

4　结论

认证测试方法是串空间模型中分析安全协议的一种重要方法,但是原有的认证测试方法受测试分量的限制,其分析范围有一定的局限性,并且在用主动测试进行分析时忽略了测试分量新鲜性的判断标准,会导致一些分析误差.

笔者主要针对以上缺陷,对原有认证测试方法进行了扩展,使之能够分析使用签名和哈希函数的协议,并增加了对测试分量新鲜性的验证,进一步完善了认证测试方法,扩大了其分析范围.通过用扩展后的认证测试方法对使用签名和哈希函数的TLS协议进行分析,发现了其中的缺陷,说明扩展后认证测试方法的有效性,同时还可以用类似的方法证明改进后的TLS协议的安全性.在认证测试的基础上实现协议的自动化验证是下一步要研究的工作.

参考文献:

[1] 王惠斌,祝跃飞,常青美.协议组合逻辑系统研究[J].郑州大学学报:理学版,2008,40(4):56-59.

[2] JOSHUA D G,FABREGA F J T. Authentication tests [J]. In:Proceedings,2000 IEEE Symposium on security and Privacy. Dakland,CA,USA:IEEE Computer Society Press,2000,10(8):16-20.

[3] GUTTMAN J D,THAYER F. Authentication tests and the structure of bundles[J]. Theoretical Compuer Science ,2002,20(15):55-60.

[4] LIU D X,LI X Y,BAY C I. An attack-finding algorithm for security protocols[J]. Journal of Computer Science and Technology,2002,22(18):32-38.

[5] 卿斯汉. 安全协议[M].北京:清华大学出版社,2005.

[6] 张岚,何良生. 串空间理论的扩展及其应用[J]. 计算机工程与应用,2006(18):136-138.

Extensions to Authentication Test and Its Application

ZHOU Qing-lei, WU Xiao-ying

(School of Information Engineering, Zhengzhou University ,Zhengzhou 450001,China)

Abstract: Authentication test method has certain limitations in analyzing the safety of security protocol because of its limited analysis area. Therefore, authentication test method based on the strand space model was extended by modifying the test component and authentication test rules to improve the method. This revised method is used for the firt time to analyze TLS protocol that included signature and hash function . It enlarged analyzing area of authentication test. Furthermore, the paper pointed out that It is necessary to check up freshment of the test segment, which makes authentication test method more perfect.

Key words: strand space model; authentication test; TLS protocol; hash function; test segment