维普资讯 http://www.cqvip.com

串空间模型中认证性测试方法的缺陷

邓珍荣[1,2]　李陶深[1]

(广西大学计算机与电子信息学院　南宁 530004)[1]　(桂林电子工业学院计算机系　桂林 541004)[2]

摘　要　指出了串空间模型中认证性测试方法存在的不足：1. 分析认证性的过程中未考虑同一协议主体同时以不同身份参与协议运行的情况；2. 分析认证性的过程中未考虑发生多轮协议同时运行的情况；3. 认证性测试方法不能分析类型错误攻击。通过实例——Needham-Schroeder 协议分析了认证性测试方法存在不足的原因，并提出了改进方案。

关键词　认证性测试方法，类型错误攻击，协议

Limitation of Authentication Tests Method Based on the Strand Space Model

DENG Zhen-Rong[1,2]　LI Tao-Shen[1]

(Colloge of Computer and Electric Information, Guangxi University, Nanning 530004)[1]

(Department of Computer, Guilin University of Electronic Technology, Guilin 541004)[2]

Abstract　The paper pointed out that authentication tests method based on the strand space model has three limitations. Firstly, during the authentication analyzing, the method has not take the same principal participate in the protocol run as different role into account. Secondly, during the authentication analyzing, the method has not take more than one of the protocol run exist at the same time into account. At last, authentication test method can not analyze type flaw attack. The paper also presented the reason of limitation through the analyzing of Needham-Schroeder protocol and given the scheme of improving authentication tests method.

Keywords　Authentication tests method, Type flaw attack, Protocol

1　引言

近年来，计算机的通信安全问题越来越受到人们关注，要保证通信信息的安全性，不仅需要良好的加密算法，也要安全的通信协议，然而，协议安全性的分析却具有很大的难度。目前，在协议安全的理论研究中，形式化的分析方法是关键的方法之一。在为形式化分析所开发的所有逻辑和模型中，串空间模型[1~3]是一个简洁而又自然的模型，以串空间模型为基础实现的模型检验器可以缓解目前所有其它模型检验器所遇到的状态空间爆炸问题[4,5]。

在串空间模型的基础上，Guttman 和 Thayer 提出了用认证性测试方法[6]来验证协议的认证性。认证性测试方法是目前唯一的一种基于串空间模型的认证性分析方法，Guttman 通过多个实例说明了该方法的简单易用性，同时也指出了该方法的一些不足[7]：认证性分析中的测试元素不能是其它消息的真子项。除此之外，我们在研究该方法的过程中，还发现认证性测试方法存在其它的不足：1、分析认证性的过程中未考虑同一协议主体同时以不同身份参与协议运行的情况；2、分析认证性的过程中未考虑多轮协议同时多轮协议运行的情况；3、认证性测试方法不能分析类型错误攻击。针对这些问题，并参考防止类型错误攻击的相关文献[8,9]，本文提出了一种改进的认证测试方法，该方法通过对正常串逐步求精，最后确定正常串之间能否存在攻击串，改进后的认证性测试方法可以分析出协议中可能存在的类型错误攻击。

2　认证性测试方法

2.1　认证性测试方法的原理

在串空间模型中进行认证性分析基于这样一个原理：在一次协议各主体的通信过程中，如果正常主体加密传输的数据未被入侵者攻击，那么它的形式(form)就不会被改变，否则，入侵者要攻击正常主体之间传输的数据，那么它就必须改变这个被传输数据的形式，即将数据加密或解密以获得其中的某些应当具有秘密性的值。根据这点，Guttman 和 Thayer 提出了三种认证性测试[6,7]，一是输出测试(outgoing test)——如果一个值 v 被加密传输出去，而后 v 又以另外的一种形式被接收了，那么就只有正常协议主体可以将它从它的加密形式中解密出来；二是输入测试(incoming test)——如果一个值 v 以一种形式被传输出去，而后 v 又以另外的一种加密的形式被接收到的，那么只能是正常的主体将它加密成这种形式的；三是主动测试(unsolicited test)，如果一个值 v 以一种全新的加密的形式被接收，那么它一定是被某个正常的主体加密的。

对于以上原理，在认证性测试方法中用以下三条定理来描述：

认证性测试 1　令 C 是一个满足 $n' \in C$ 的束，且 $n \Rightarrow^+ n'$ 为 a 在 t 中的一个输出测试边，那么：

i. 存在正常结点 $m, m' \in C$ 使得 t 是 m 的一个元素；且对于 a 来说，$m \Rightarrow^+ m'$ 是一条前变形边(transforming edge)。

ii. 假设增加条件：a 只在 m' 的元素 $t_1 = \{|h|\}_{K_1}$ 中出现，其中的 t_1 不是任何正常元素的真子项，且 $K_1^{-1} \notin P$，那么存在一个负的正常结点，在这个结点中 t_1 是它的一个元素。

认证性测试 2　令 C 是一个满足 $n' \in C$ 的束，且令 $n \Rightarrow^+ n'$ 为 a 在 t 中的一个输入测试边，那么存在两个正常结点 m，$m' \in C$ 使得 t' 是 m' 的一个元素，且对于 a 来说，$m \Rightarrow^+ m'$ 是一

维普资讯 http://www.cqvip.com

条前变形边。

认证性测试 3 C 是一个束，$n\in C$，且 n 是 $t=\{|h|\}_K$ 的一个主动测试，那么必然存在一个正常的正结点 $m\in C$ 使得 t 是 m 的一个元素。

2.2 认证性测试方法的应用——Needham-Schroeder 协议的认证性分析

Needham-Schroeder 协议（简称 NS 协议）设计的初衷是两个协议主体（发起方 A 和应答方 B）之间利用利用临时值相互认证对方的身份。

NS 协议的标准描述如下：

$A\rightarrow B:\{A,N_a\}_{K_B}$

$B\rightarrow A:\{N_a,N_b\}_{K_A}$

$A\rightarrow B:\{N_b\}_{K_B}$

NS 协议中包含两种类型的正常串：

发起方串具有以下迹：$\langle+\{A,N_a\}_{K_B},-\{N_a,N_b\}_{K_A},+\{N_b\}_{K_B}\rangle$

其中 $A\in T_{name}$，$N_a,N_b\in T$，且 $N_a\notin T_{name}$，我们用 $Init[A,B,N_a,N_b]$ 来记录所有满足以上迹的串的集合。

应答方串具有以下迹：$\langle-\{A,N_a\}_{K_B},+\{N_a,N_b\}_{K_A},-\{N_b\}_{K_B}\rangle$

其中 $A\in T_{name}$，$N_a,N_b\in T$，且 $N_b\notin T_{name}$，我们用 $Resp[A,B,N_a,N_b]$ 来记录所有满足以上迹的串的集合。

在文[6]中，Guttman 利用认证性测试的方法证明了 NS 协议的认证性结果。

结果 1：给定一个束 C，C 中包含一个串 $s_r\in Resp[A,B,N_a,N_b]$，s_r 的 C_height 为 3，并且假设 $K_A^{-1}\notin K_p$、$N_a\neq N_b$ 以及 N_b 只有唯一的生成点，那么在束 C 中就必然存在一个 C_height 为 3 的发起方串 $s_i\in Init[A,B',N_a,N_b]$。

证明：s_r 的第二个结点$\langle s_r,2\rangle$和第三个结点$\langle s_r,3\rangle$形成了一个对 N_b 的输出测试，又因为$\langle s_r,2\rangle$中的$\{N_aN_b\}_{K_A}$包含 N_b，$\{N_aN_b\}_{K_A}$ 不是任何其它正常结点的真子项，所以 $\{N_aN_b\}_{K_A}$ 是关于 N_b 的测试元素。检查其它前提条件，可知 $\langle s_r,2\rangle\Rightarrow^+\langle s_r,3\rangle$ 是 N_b 的一个输出测试，测试元素为 $\{N_aN_b\}_{K_A}$。根据认证性测试 1，在束 C 中必然存在正常结点 m' 满足：$\{N_aN_b\}_{K_A}$ 是 m 的一个元素，且 $m\Rightarrow^+m'$ 是关于 N_b 的前变形边。因为 m 是一个负结点，且 $\{N_aN_b\}_{K_A}=term(m)$，所以 m 是某个发起方串 $s'_i\in Init[A',B',N'_a,N'_b]$ 的 $\langle s'_i,2\rangle$，又因为 $term(\langle s'_i,2\rangle)=\{N_aN_b\}_{K_A}$，由此得出 $A=A'$、$N_a=N'_a$、$N_b=N'_b$。所以，在包含应答方串的束 C 中一定包含一个满足 $s'_i\in Init[A,B',N_a,N_b]$ 的发起方串。根据这个证明结果，对于应答方 B 来说，他本来期望与他通信的发起方满足串 $s_i\in Init[A,B,N_a,N_b]$ 的要求，而发起方却可以用满足 $s'_i\in Init[A,B',N_a,N_b]$ 的串来欺骗他。

结果 2：给定一个束 C，C 中包含一个串 $s_i\in Init[A,B,N_a,N_b]$，s_i 的 C_height 为 3，并且假设 $K_A^{-1},K_B^{-1}\notin K_p$ 以及 N_a 只有唯一的生成点，那么在束 C 中就必然存在一个 C_height 为 2 的发起方串 $s_r\in Resp[A,B,N_a,N_b]$。

认证性结果 2 的证明过程参见文[6]。

NS 协议的认证性结果表明，NS 协议中存在一类攻击。这类攻击就是：对于参与协议的正常应答者 B 来说，与它通信的发起方串不是 $s_i\in Init[A,B,N_a,N_b]$，而是 $s'_i\in Init[A,B',N_a,N_b]$，这类攻击实际上就是与其它文[10]结论一致的中间人攻击（见图 1）。

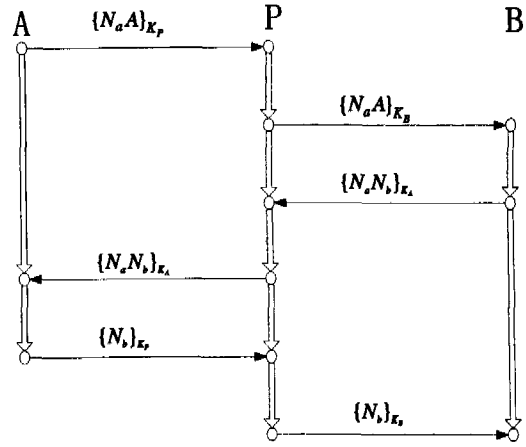

图 1　NS 协议的中间人攻击

3　认证性测试方法的问题

在文[11]中，作者指出了 NS 协议中存在的另外一种攻击——类型错误攻击（见图 2）。为什么应用认证性测试方法不能发现类型错误攻击呢？考察以上对 NS 协议的分析过程，就可以发现认证性测试方法不能发现类型错误攻击的原因有两方面：第一方面，分析过程的问题，认证性测试方法中未考虑同一个协议参与者同时以一种以上的角色参与协议的情况，也未考虑同一主体同时参与多轮协议运行的情况。如以上提到的 NS 协议的类型错误攻击，就是 B 同时参与了两轮协议的运行；第二方面，串空间模型的问题，因为串空间模型中描述消息的时候并不指定该消息的类型，所以认证性测试方法不能区别接收到的消息的类型，这就给类型错误攻击的攻击者提供了可乘之机。

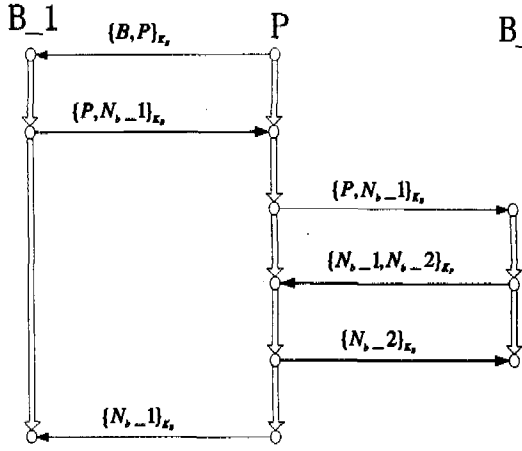

图 2　NS 协议的类型错误攻击

首先我们来看第一方面的原因。在图 2 中，应答方 B 可以同时参与多轮协议运行，用 B_1 标志 B 参与第一轮协议运行（相应的串为 S_{B_1}），B_2 标志 B 参与第二轮协议运行（相应的串为 S_{B_2}），N_b_1 是 B 参与第一轮协议时产生的临时值，N_b_2 是 B 参与第二轮协议时产生的临时值。

对于参与第一轮协议的 B_1 来说，他在$\langle S_{B_1},2\rangle$发出了包含 N_b_1 的$\{P,N_b_1\}_{K_B}$，然后又在$\langle S_{B_1},3\rangle$接收到了包含 N_b_1 的$\{N_b_1\}_{K_B}$，再检查其它的前提条件，可知$\langle S_{B_1},2\rangle\Rightarrow^+\langle S_{B_1},3\rangle$形成了一个对 N_b_1 的输出认证性测试，测试元素为$\{P,N_b_1\}_{K_B}$。如此根据认证性测试 1，在束 C 中必然存在正常结点 m' 满足：$\{P,N_b\_1\}_{K_B}$ 是 m 的一个元素，且 $m\Rightarrow^+m'$ 是关于 N_b_1 的前变形边，且$\{P,N_b_1\}_{K_B}$是 m 的一

维普资讯 http://www.cqvip.com

个元素。在 Guttman 等人的 NS 协议的证明中，由以上条件便直接推出了这个包含$\{P,N_b\ 1\}_{K_B}$的 m 结点便是某个发起方串的第二个结点，也就是认为$\{P,N_b\ 1\}_{K_B}$的解密工作是由发起方完成的，实际上在这里，$\{P,N_b\ 1\}_{K_B}$只是由发起方直接重放了一次，最后真正的解密操作是由参与第二轮协议运行的应答方 $B\ 1$ 来完成的。

再来看第二方面的原因，在 $B\ 1$ 发出的$\{P,N_b\ 1\}_{K_B}$中，P 是作为发起方的临时值参与协议运行的，但是当 $B\ 2$ 接收到$\{P,N_b\ 1\}_{K_B}$时，P 却是作为一个主体名参与协议运行的。如果 $B\ 1$ 在发送$\{P,N_b\ 1\}_{K_B}$的时候指定了各个消息值的类型，$B\ 2$ 在接收到$\{P,N_b\ 1\}_{K_B}$是就会发现 P 的类型与自己应该接收的值类型不一致，从而发现攻击的存在。

4 认证性测试方法的改进

假设 princ(n)=Q(princ 的定义请参见文[12])，即结点 n 的运行主体是 Q。在应用认证性测试 1 的过程中，满足条件的前变形边 $m\Rightarrow^{+}m'$可能属于除 Q 外的其他正常主体，也可能属于 Q。若 $m\Rightarrow^{+}m'$属于 Q，则证明过程同文[6,7]。若 $m\Rightarrow^{+}m'$属于 Q 之外的其他主体，则需作如下检查：

如果遵循协议规则运行的 Q 中存在前变形边 $t\Rightarrow^{+}t'$，且 t 中各个子项的长度都与 m 中各个子项的长度相同，那么就需检验该协议中是否存在类型错误攻击，也就是 n 中的加密元素 $t_1=\{|h|\}_{K_1}$可能是由发送该元素的主体解密的。

这种攻击是否存在就要通过以下四个步骤来证明：

1. 确定 Q 第一次运行的迹，即 $n\Rightarrow^{+}n'$所在的串；

2. 假设 $t\Rightarrow^{+}t'$就是 $m\Rightarrow^{+}m'$，确定 Q 第二次运行的迹；

3. 反复比较 Q 的第一次运行的迹和第二次运行的迹，比较的过程中尽可能多地确定两种迹中尚未明确的消息项；

4. 由最后的两个迹确定是否存在攻击。

例如以上的 NS 协议，分析完中间人攻击后，我们再检查，发现协议主体 B 的迹中含有前变形边$\langle s_B,1\rangle\Rightarrow^{+}\langle s_B,2\rangle$，且$\langle s_B,1\rangle$与输出测试边$\langle s_B,2\rangle\Rightarrow^{+}\langle S_{B,3}\rangle$中的$\langle s_B,2\rangle$各个子项的长度都相同，因此符合需要检测是否存在类型错误攻击的条件，下面作具体的分析：

假设 B 的第一次运行的串为 s_1，第二次运行的串为 s_2。根据协议和认证性测试 1，串 s_1 中含有关于 N_b 的输出测试边，所以

$$s_1=\langle -\{X_1,X_2\}_{K_B},+\{X_2,N_b\}_{K_{X_1}},-\{N_b\}_{K_B}\rangle \quad (1)$$

因为 s_2 中只有$\langle s_2,1\rangle\Rightarrow^{+}\langle s_2,2\rangle$能形成前变形边，且该前变形边必然是关于 N_b 的前变形边，所以得出

$$s_2=\langle -\{X_3,N_b\}_{K_B},+\{N_b,X_4\}_{K_{X_3}},-\{X_4\}_{K_B}\rangle \quad (2)$$

因为$\langle s_1,2\rangle$发出$\{X_2,N_b\}_{K_{X_1}}$后是由$\langle s_2,1\rangle\Rightarrow^{+}\langle s_2,2\rangle$来变形的，其它的攻击者不能对$\{X_2,N_b\}_{K_{X_1}}$进行加解密操作，所以$\langle s_2,1\rangle$中必然包含$\{X_2,N_b\}_{K_{X_1}}$，又因为$\langle s_2,1\rangle=-\{X_3,N_b\}_{K_B}$，所以$\langle s_2,1\rangle=\langle s_1,2\rangle$，$s_1$、$s_2$ 修改为：

$$s_1=\langle -\{X_1,X_2\}_{K_B},+\{X_2,N_b\}_{K_B},\{N_b\}_{K_B}\rangle \quad (3)$$

$$s_2=\langle -\{X_2,N_b\}_{K_B},+\{N_b,X_4\}_{K_{X_3}},-\{X_4\}_{K_B} \quad (4)$$

根据协议，串 s_1 中$\langle s_1,1\rangle$中的 X_1 与$\langle s_1,2\rangle$中的加密密钥对应的主体名相同，串 s_2 中$\langle s_2,1\rangle$中的 X_1 与$\langle s_2,2\rangle$中的加密密钥对应的主体名相同，所以

$$s_1=\langle -\{B,X_2\}_{K_B},+\{X_2,N_b\}_{K_B},-\{N_b\}_{K_B}\rangle \quad (5)$$

$$s_2=\langle -\{X_2,N_b\}_{K_B},+\{N_b,X_4\}_{K_{X_2}},-\{X_4\}_{K_B}\rangle \quad (6)$$

根据协议，X_4 是 s_2 中主体所生成的临时值，又根据串$\langle s_2,1\rangle$和$\langle s_2,3\rangle$中的加密密钥为 K_B，所以 s_2 的主体为名为 B，因此

$$s_2=\langle -\{X_2,N_b\}_{K_B},+\{N_b,N'_b\}_{K_{X_2}},-\{N'_b\}_{K_B}\rangle \quad (7)$$

式(5)和(7)分别是最后求得的 s_1 和 s_2 的结果。串如果攻击存在的话，下面我们便可以逐步给出攻击者的迹。

协议运行起来后，s_1 和 s_2 都在开始就接收到了未知信息 X_2，在假设攻击者的初始已知信息中不包括正常主体的私钥和正常主体生成的临时值的情况下，那么就只有$\langle s_1,1\rangle$是来自攻击者的，当攻击者发出$-\{B,X_2\}_{K_B}$后，正常主体 B 运行，B 在$\langle s_1,2\rangle$发出了用于验证对方身份的消息$\{X_2,N_b\}_{K_B}$，由于攻击者假冒了 B 与 B 进行通信，因此该验证消息最后又发给了 B，这就引起了 B 参与第二轮协议运行，最后参与第二轮协议运行的 B 为第一轮协议运行的攻击者解密了所需的临时值 N_b。但至此，攻击者仍然不知道任何需要保密的值，所以他需要参与第二轮协议运行的 B 的解密结果。我们再来看 s_2，从 s_2 的迹可以看出，参与第二轮协议运行的 B 是在跟一个未知主体 X_2 进行通信，而这个 X_2 是在最开始的时候由攻击者提供给参与第一轮协议运行的主体 B 的，也就是说，参与第二轮协议运行的 B 到底把解密后消息发给谁是由攻击者决定的，如此一来，只要攻击者将 X_2 定为他自己的主体名，攻击者就可以从参与第二轮协议运行的 B 那里获得所需的值 N_b 和 N'_b。所以最后得出攻击者的迹：$\langle +\{B,P\}_{K_B},-\{P,N_b\}_{K_B},+\{P,N_b\}_{K_B},-\{N_b,N'_b\}_{K_p},+\{N'_b\}_{K_B},+\{N_b\}_{K_B}\rangle$。

至此，改进后的方法分析出了原方法所未能分析出的类型错误攻击。

结束语 本文通过对应用认证性测试方法对 NS 协议进行分析，分析后的结果表明认证性测试方法不能分析出 NS 中的类型错误攻击。本文采用对正常串逐步求精的思想，通过扩充改进认证性测试方法，最后分析出了 NS 协议中的类型错误攻击。串空间模型是基于定理证明思想开发的，而本文采用的逐步求精依据的也是一种数学思想，因此，笔者认为该逐步求精和串空间模型是可以很自然地结合的，深入研究逐步求精思想在串空间模型中的应用是下一步要进行的工作。

参 考 文 献

1 Thayer F, Herzog J C, Guttman J D. Strand spaces: why is a security protocol correct? In: Proc. of 1998 IEEE symposium on Security and Privacy, 1998

2 Thayer F, Herzog J C, Guttman J D. Strand Spaces: [Technical Report]. The MITRE Corporation, Nov. 1997

3 Thayer F, Herzog J C, Guttman J D. Honest Ideals on Strand Spaces. In: Proc. of the 1998 IEEE Computer Security Foundations Workshop, IEEE Computer Society Press, 1998. 66～77

4 Song D, Berezin S, Perrig A. Athena: A novel approach to efficient automatic security protocol analysis. Journal of Computer Security, 2001, 9(1-2): 47～74

5 范红，冯登国. 安全协议理论与方法. 科学出版社，2003

6 Guttman J D, Fábrega E J T. Authentication test and the structure of Bundles. The MITRE Corporation, Feb. 2000

7 Guttman J D, Fábrega F J T. Authentication tests. In: Proc. 2000 IEEE Symp. Security ans Privacy, IEEE Computer Society Press, Berkeley, California, May 2000. 96～109

8 Heathen J, Lowe G, Schneider S. How to prevent type flaw attacks on security protocols. In: Proc. of 13th IEEE Computer Security Foundations Workshop, 2000. 255～268

9 Li Yafen, Yang W, Huang C W. Preventing type flaw attacks on security protocols with a simplified tagging scheme. Journal of Information Science and Engineering, (NSC 92-2213-E-009-070). July 2004

10 Lowe G. An attack on the Needham-Schroeder public key authentication protocol. Information Processing Letters, 1995, 56: 131～136

11 张玉清，朱宏儒，肖国镇. 密码协议的 SMV 分析：实例研究. 计算机工程，1999, 25: 156～158

12 Abadi M, Tuttle M R. A semantics for a logic of authentication. In: Proc. of the 10th ACM Symposium on Principles of Distributed Computing. ACM Press, 1991. 201～216