# 一个双向认证协议的分析与改进

廖振岚 吴开贵 谢 琪 代廷合
(重庆大学计算机学院 重庆 400043)

**摘 要** 运用安全协议形式化分析方法中的串空间模型理论,对 Natalia Miloslavskaya 等人提出的一个双向认证协议进行了分析,发现该协议在认证方面存在缺陷,并对该协议进行了改进,同时用串空间理论证明了改进后的协议的认证正确性。

**关键词** 安全协议,认证,串空间
**中图法分类号** TP393 **文献标识码** A

## Analysis and Improvement of a Mutual Authentication Protocol

LIAO Zhen-lan WU Kai-gui XIE Qi DAI Ting-he
(College of Computer Science of Chongqing University, Chongqing 400043, China)

**Abstract** This paper applied strand space model, which is a method for formal analysis of security protocol, to analyse a mutual authentication protocol proposed by Natalia Miloslavskaya et al., and found some flaws of the protocol on authentication. Then an improved protocol was proposed, and its correctness on authentication was proved by using strand space model.

**Keywords** Security protocol, Authentication, Strand space

## 1 引言

作为网络安全的重要组成部分,安全协议在现实中得到了非常广泛的应用。随着新系统和新应用的不断涌现,已有的安全协议已经不能满足需求。为了适应新的环境,人们设计出许多新的安全协议,尽管都经过精心设计,但是仍然存在错误,因此需要对协议进行仔细的分析。

安全协议分析可分为形式化分析和非形式化分析,其中形式化分析方法是安全协议理论研究的热点之一。常见的形式化分析方法有 BAN 逻辑[1]、Kailar 逻辑[2]、SPI 演算[3,4]、CSP 方法[5]、串空间模型[6,7]等。本文采用了串空间模型理论来进行协议分析,它是在 1998 年由 Thayer, Herzog 和 Guttman 提出的,具有高效、直观、实用等特点,不仅可以用于证明安全协议的正确性,还可以用于构造攻击,揭示安全协议的内在缺陷。该方法已经成功地分析了 Needham-Schroeder-Lowe 协议[6]、Otway-Rees 协议[7]、Yahalom 协议[8]、802.11i[9] 协议等诸多协议,被公认为是一种先进的、高效的协议分析方法。

## 2 Natalia Miloslavskaya 提出的认证协议[10]

Natalia Miloslavskaya, Alexander Tolstoy 和 Dmitriy Ushakov 在 2007 年提出一个新的双向认证协议[10](我们称它为 NAD 认证协议),主要目的在于为动态的分布式信息系统提供透明和可靠的认证,并且希望它能够比传统的认证协议提供更大的灵活性以及更好的运行性能。该协议的基础是公钥密码体制和数字签名,核心思想是以私钥签名来确认消息发送者的身份,以代理证书作为授权机制。它由以下 7 个回合构成。

(1) $A \rightarrow AS: A$

(2) $AS \rightarrow A: \{N_{as}\}_{-Kas}$

(3) $A \rightarrow AS: \{N_a\}_{-Ka}, \{F_1(N_{as})\}_{-Ka}$

(4) $AS \rightarrow A: \{F_2(N_a)\}_{-Kas}, CertA$

(5) $A \rightarrow IS: CertA, \{A, N_{a2}\}_{-Ka}$

(6) $IS \rightarrow A: \{F_3(N_{a2})\}_{-Kis}, \{N_{is}\}_{-Kis}$

(7) $A \rightarrow IS: \{F_4(N_{is})\}_{-Ka}$

其中符号的含义如下:

$A$ —客户标识符(数字或名字,能够让身份认证服务器确认客户身份的任意标识符);

$AS, IS$—身份认证服务器、信息服务器;

$N_x$—由协议参与主体 $X$ 生成的随机数;

$F_x(N_y)$—在大部分情况下,这是一个带有一个自变量的可逆函数(也可以是一个单向函数),比如 $F_x = N_y - 1$;

$-Kx, +Kx$ —主体 $X$ 的私钥和公钥($X = A, IS$ 或 $AS$);

$\{X\}_{-Ky}$—用私钥 $-Ky$ 对 $X$ 消息签名;

$CertA$—客户 $A$ 的代理证书。实际内容为 $\{A, +KA, AS, Time\}_{-Kas}$,其中 $Time$ 为证书的生存时间。

协议的目的是通信各方之间相互的身份认证。从逻辑上

到稿日期:2008-04-15 本文受国家自然科学基金资助项目(30400446)资助。
廖振岚 硕士生,主要研究方向为网络安全,E-mail:liaozhenlan_2008@163.com;吴开贵 副教授,主要研究方向为计算机安全技术;谢 琪 硕士生,主要研究方向为网络安全;代廷合 硕士生,主要研究方向为网络安全。

看，前 4 个协议回合是客户与身份认证服务器之间的相互认证，后 3 个回合是客户与信息服务器之间的相互认证。其中，证书的主要作用是授权客户 $A$ 以一定的权限与信息服务器通信。

如前所述，在逻辑上可以把前 4 个回合与后 3 个回合分开，为了方便，本文把 NAD 协议当作由两个部分组成：前 4 个回合作为第一部分，称为 NAD Part Ⅰ；后 3 个回合作为第二部分，称为 NAD Part Ⅱ。

## 3 串空间模型的符号说明

在串空间中，一个串代表了一个协议主体在唯一的一次协议运行中的所有事件，一个丛代表了协议唯一的一次运行，是所有参与此次协议运行的主体所对应的串的集合。如果协议在认证方面是正确的，那么每个丛都包含了所有合法协议主体所对应的串，这些串在通信主体、随机数、会话密钥等数据上是一致的[6]。举例来说，如果一个协议有 3 个合法的协议主体：发起者 $A$，响应者 $B$，服务器 $S$，但在某个丛中仅包含了两个合法协议主体的串，比如是 $A$ 的串和 $S$ 的串，也就说明了有入侵者 $P$ 冒充 $B$ 与 $A$，$S$ 完成了协议，而 $A$，$S$ 并没有发觉，这显然是认证出了问题。另一情况是丛中包含了 $A$，$B$，$S$ 的串，$A$，$S$ 认为是 $A$，$B$，$S$ 在通信，$B$ 却认为是 $P$，$B$，$S$ 在通信，这说明了 $A$，$B$，$S$ 没有对参与协议的通信主体达成一致认识，协议的认证性有缺陷。

串空间模型是一套完整的形式化的协议分析理论[1]。本文所使用的符号与文献[6]相似。集合 $\mathcal{A}$ 中的元素为协议主体交换的消息，它的构造如下：

(1)$\mathcal{T}\subseteq\mathcal{A}$ 是正文消息，表示原子消息。其中，$\mathcal{T}_{name}$ 是协议主体标识符的集合。

(2)$\mathcal{K}\subseteq\mathcal{A}$ 是密钥的集合，$\mathcal{K}$ 与 $\mathcal{T}$ 是不相交集。其中，$\mathcal{K}_p$ 是入侵者所拥有的密钥的集合。

(3)两个二元算子

$encr:\mathcal{K}\times\mathcal{A}\mapsto\mathcal{A}$

$join:\mathcal{A}\times\mathcal{A}\mapsto\mathcal{A}$

根据传统习惯将 $encr(K,m)$ 写成 $\{m\}K$，将 $join(a,b)$ 写成 $ab$。

采用串空间模型，可对 NAD 协议进行形式化描述(如图 1 所示)，其符号说明如下：

$A,AS,IS\in\mathcal{T}_{name}$，$N_a,N_{as},N_{is}\in\mathcal{T}\setminus\mathcal{T}_{name}$

$-K_{as},-K_a,-K_{is}\in\mathcal{K}$

$CertA\in\mathcal{A}$

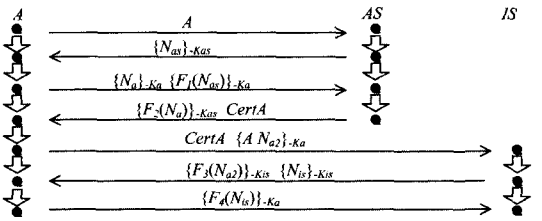


图 1 NAD 协议的消息交换

## 4 NAD 协议的分析

下面将对协议进行具体分析。为了简化证明过程，先引入一个引理，具体证明见文献[11]。

**引理 1** 如果 $\{h\}_K$ 作为结点 $n$ 的一个子项出现在丛 $C$ 中，其中 $h\in\mathcal{A}$，$K\in\mathcal{K}\setminus\mathcal{K}p$，那么 $\{h\}_K$ 起源于一个正则结点 $m$。

### 4.1 NAD Part Ⅰ的分析

NAD Part Ⅰ的渗透串空间由下述 3 种串组成：

(1)攻击者串 $s\in\mathcal{P}$，其中 $\mathcal{P}$ 为攻击者串的集合。

(2)发起者串 $s\in Init[A,AS,N_a,N_{as},CertA]$，其迹为 $\langle+A,-\{N_{as}\}_{-Kas},+\{N_a\}_{-Ka}\{F_1(N_{as})\}_{-Ka},-\{F_2(N_a)\}_{-Kas}CertA\rangle$

$Init[A,AS,N_a,N_{as},CertA]$ 表示了所有具有上述迹的串的集合，与这种串对应的主体是 $A$。

(3)服务器串 $S\in Serv[A,AS,N_a,N_{as},CertA]$，其迹为 $\langle-A,+\{N_{as}\}_{-Kas},-\{N_a\}_{-Ka}\{F_1(N_{as})\}_{-Ka},+\{F_2(N_a)\}_{-Kas}CertA\rangle$

$Serv[A,AS,N_a,N_{as},CertA]$ 表示了所有具有上述迹的串的集合，与这种串对应的主体是某一个固定的认证服务器 $AS_0$。

#### 4.1.1 服务器的保证

**命题 1** 假设下列条件成立：

(1)$\sum$是 NAD Part Ⅰ的串空间，$C$ 是 $\sum$ 中的一个丛，$s$ 是一个 $Serv[A,AS,N_a,N_{as},CertA]$ 中的服务器串，且 $C-height(s)=4$；

(2)$-K_a\notin\mathcal{K}_p$；

(3)$N_{as}$ 在 $\sum$ 中是惟一起源的项；

(4)对于任意一个认证服务器 $AS'$，有 $-K_{as}'\notin\mathcal{K}_p$。

于是，$C$ 中包含一个发起者串 $t\in Init[A,AS,*,N_{as},*]$，且 $C-height(t)=3$。

证明：$\{F_1(N_{as})\}_{-Ka}$ 作为一个子项出现在结点 $\langle s,3\rangle$ 上，$-Ka\notin\mathcal{K}_p$，由引理 1 知 $\{F_1(N_{as})\}_{-Ka}$ 起源于一个正则结点 $m$，，经观察，$m$ 在发起者串 $t\in Init[A,AS',*,N_{as},*]$ 上，$m=\langle t,3\rangle$。则有 $term(\langle t,2\rangle)=\{N_{as}\}_{-Kas'}$。由条件 4 及引理 1，可推出 $\{N_{as}\}_{-Kas'}$ 出现在某个正则串 $s'\in Serv[*,AS',*,N_{as},*]$ 上。从服务器串的形式得知 $N_{as}$ 起源于 $s'$，而 $N_{as}$ 又惟一起源于 $s$，所以 $s'=s$，进而得到 $AS'=AS$。所以，有 $t\in Init[A,AS,*,N_{as},*]$。$m$ 是 $t$ 的第三个结点，故有 $C-height(t)=3$。

#### 4.1.2 发起者的保证

**命题 2** 假设下列条件成立：

(1)$\sum$是 NAD Part Ⅰ的串空间，$C$ 是 $\sum$ 中的一个丛，$t$ 是一个 $Init[A,AS,N_a,N_{as},CertA]$ 中的发起者串，且 $C-height(t)=4$；

(2)$-K_{as}\notin\mathcal{K}_p$；

(3)$N_a$ 在 $\sum$ 中是惟一起源的项。

于是，$C$ 中包含一个服务器串 $s\in Serv[*,AS,N_a,*,*]$，且 $C-height(s)=4$。

证明：$\{F_2(N_a)\}_{-Kas}$ 作为一个子项出现在结点 $\langle t,4\rangle$ 上，$-K_{as}\notin\mathcal{K}_p$，由引理 1 知 $\{F_2(N_a)\}_{-Kas}$ 起源于一个正则结点 $m$。经观察，$m$ 在服务器串 $s\in Serv[*,AS,N_a,*,*]$ 上，$m=\langle s,4\rangle$，$C-height(s)=4$。

### 4.2 NAD Part Ⅰ的缺陷以及出现缺陷的原因

在命题 1 中，证明的结果表明：如果认证服务器 $AS$ 正确地执行一轮协议，那么 $AS$ 就认为它与 $A$ 完成了一轮协议，而 $A$ 也认为它跟 $AS$ 执行了一轮协议。换言之，$AS$ 能认证 $A$。

在命题 2 中，证明的结果表明：如果客户 $A$ 正确地执行

一轮协议，那么 $A$ 就认为它与 $AS$ 完成了一轮协议，然而 $AS$ 认为它没有跟 $A$ 进行通信。一种可能出现的攻击过程如下：

(1)$A\rightarrow P(AS):A$

1)$P\rightarrow AS:P$

2)$AS\rightarrow P:\{N_{as}\}_{-Kas}$

(2)$P(AS)\rightarrow A:\{N_{as}\}_{-Kas}$

(3)$A\rightarrow P(AS):\{N_a\}_{-Ka},\{F_1(N_{as})\}_{-Ka}$

3)$P\rightarrow AS:\{N_a\}_{-Kp},\{F_1(N_{as})\}_{-Kp}$

4)$AS\rightarrow P:\{F_2(N_a)\}_{-Kas},CertP$

(4)$P(AS)\rightarrow A:\{F_2(N_a)\}_{-Kas}$ *

为什么 $AS$ 能认证 $A$ 而 $A$ 却不能认证 $AS$？命题 1 中，存在一个假设：所有的身份认证服务器都是诚实的、合法的，他们的私钥也没有泄露。有了这个假设，服务器的一致性得到了保证。而在命题 2 中，如果想得到与命题 1 类似的结论，必须增加一个类似假设：所有的客户都是诚实的、合法的，他们的私钥也没有泄露。这个假设明显是不合理的。对于攻击者来说，获得一个合法的身份认证服务器身份是很困难的，而获得一个合法的客户身份相对而言并不困难。

### 4.3 NAD Part Ⅱ的分析

NAD Part Ⅱ的分析过程以及分析结果与 NAD Part Ⅰ十分相似，此处仅给出对 NAD Part Ⅱ的攻击过程：

(1)$A\rightarrow P(IS):CertA,\{A,N_{a2}\}_{-Ka}$

1)$P\rightarrow IS:CertP,\{P,N_{a2}\}_{-Kp}$

2)$IS\rightarrow P:\{F_3(N_{a2})\}_{-Kis},\{N_{is}\}_{-Kis}$

(2)$P(IS)\rightarrow A:\{F_3(N_{a2})\}_{-Kis},\{N_{is}\}_{-Kis}$

(3)$A\rightarrow P(IS):\{F_4(N_{is})\}_{-Ka}$

3)$P\rightarrow IS:\{F_4(N_{is})\}_{-Kp}$

## 5 对 NAD 协议的改进

本文参照 ISO three-pass 双方公钥认证协议对 NAD 协议进行了改进，同样把改进后的协议分为 Part Ⅰ和 Part Ⅱ两部分：

(1)$A\rightarrow AS:A$

(2)$AS\rightarrow A:N_{as}$

(3)$A\rightarrow AS:\{N_{as},N_a,AS\}_{-Ka}$

(4)$AS\rightarrow A:\{N_a,A\}_{-Kas},CertA$

(5)$A\rightarrow IS:CertA,N_{a2}$

(6)$IS\rightarrow A:\{N_{a2},N_{is},A\}_{-Kis}$

(7)$A\rightarrow IS:\{N_{is},IS\}_{-Ka}$

改进后的协议基本上保留了原协议的特点，而在安全上有了很大的提高。采用串空间模型，改进后的 NAD 协议可形式化描述，如图 2 所示。

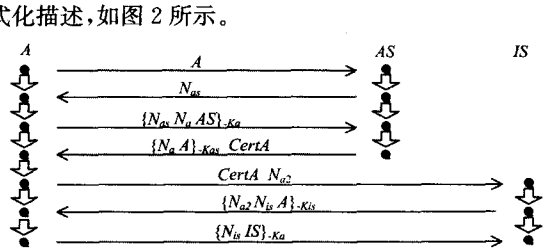


图 2 改进后的 NAD 协议的消息交换

### 5.1 改进的 NAD Part Ⅰ的分析

改进的 NAD Part Ⅰ的渗透串空间由下述 3 种串组成：

(1)攻击者串 $s\in\mathcal{P}$

(2)发起者串 $s\in Init[A,AS,N_a,N_{as},CertA]$，其迹为$\langle+A,-N_{as},+\{N_{as},N_a,AS\}_{-Ka},-\{N_a,A\}_{-Kas}CertA\rangle$

$Init[A,AS,N_a,N_{as},CertA]$表示了所有具有上述迹的串的集合，与这种串对应的主体是 $A$。

(3)服务器串 $s\in Serv[A,AS,N_a,N_{as},CertA]$，其迹为$\langle-A,+N_{as},-\{N_{as},N_a,AS\}_{-Ka},+\{N_a,A\}_{-Kas}CertA\rangle$

$Serv[A,AS,N_a,N_{as},CertA]$表示了所有具有上述迹的串的集合，与这种串对应的主体是某一个固定的认证服务器 $AS_0$。

#### 5.1.1 服务器的保证

**命题 3** 假设下列条件成立：

(1)$\sum$是改进的 NAD Part Ⅰ的串空间，$C$ 是$\sum$中的一个丛，$s$ 是一个 $Serv[A,AS,N_a,N_{as},CertA]$ 中的服务器串，且 $C-height(s)=4$；

(2)$-K_a\notin\mathcal{K}_p$；

(3)$N_{as}$在$\sum$中是惟一起源的项。

于是，$C$ 中包含一个发起者串 $t\in Init[A,AS,N_a,N_{as},*]$，且 $C-height(t)=3$。

证明：$\{N_{as},N_a,AS\}_{-Ka}$作为一个子项出现在结点$\langle s,3\rangle$上，$-K_a\notin\mathcal{K}_p$，由引理 1 知$\{N_{as},N_a,AS\}_{-Ka}$起源于一个正则结点 $m$。经观察，$m$ 在发起者串 $t\in Init[A,AS,N_a,N_{as},*]$上，$m=\langle t,3\rangle$，$C-height(t)=3$。

#### 5.1.2 发起者的保证

**命题 4** 假设下列条件成立：

(1)$\sum$是改进的 NAD Part Ⅰ的串空间，$C$ 是$\sum$中的一个丛，$t$ 是一个 $Init[A,AS,N_a,N_{as},CertA]$ 中的发起者串，且 $C-height(t)=4$；

(2)$-K_{as}\notin\mathcal{K}p,-K_a\notin\mathcal{K}p$；

(3)$N_a$ 在$\sum$中是惟一起源的项。

于是，$C$ 中包含一个服务器串 $s\in Serv[A,AS,N_a,N_{as},*]$，且 $C-height(s)=4$。

证明：$\{N_a,A\}_{-Kas}$作为一个子项出现在结点$\langle t,4\rangle$上，$-K_{as}\notin\mathcal{K}_p$，由引理 1 知$\{N_a,A\}_{-Kas}$起源于一个正则结点 $m$。经观察，$m$ 在服务器串 $s\in Serv[A,AS,N_a,N_{as}',*]$上，$m=\langle s,4\rangle$。$term(\langle s,3\rangle)=\{N_{as}',N_a,AS\}_{-Ka}$，$-K_a\notin\mathcal{K}p$，由引理 1 知$\{N_{as}',N_a,AS\}_{-Ka}$起源于一个正则结点 $n$。经观察，$n$ 在发起者串 $t'\in Init[A,AS,N_a,N_{as}',*]$上，因为 $N_a$ 惟一起源于 $t$，所以 $t'=t$，进而得到 $N_{as}'=N_{as}$。所以，$s\in Serv[A,AS,N_a,N_{as},*]$，$m$ 是 $s$ 的最后一个结点，故有 $C-height(s)=4$。

### 5.2 改进的 NAD Part Ⅱ的分析

改进的 NAD Part Ⅱ的分析过程以及分析结果与 Part Ⅰ十分相似。

**结束语** 本文对 Natalia Miloslavskaya 等人提出的一个双向认证协议进行了形式化的分析，发现该协议存在的缺陷，不能实现它的认证目标。对此，本文提出了改进的协议，并对其进行形式化的分析，证明它的正确性。改进后的协议保留了原协议的特点，而且在安全上有了很大的提高。原协议在服务器的一致性保证上，需要一个严格的条件：所有的服务器都是诚实的、合法的，改进后的协议则不需要这个条件。原协议在发起者的一致性保证上存在缺陷，改进后的协议则保证了发起者的一致性。因此，对原协议的改进是很有效果的。

（下转第 151 页）

中紧密接近图利用结构中属性域作为节点，连接节点的边利用两节点相继访问之间的“基本块”数目作为权值。

文献[10]介绍了我们在前期的工作中提出的一种简单的变量关系模型，用于支持数组重组这种数据重组方法。本文是在这方面的进一步工作，不同之处主要体现在下面的几个方面：(1)变量关系图相比于变量关系模型更加精确，增加了复用距离的值对差异程度的影响因子，引入了访问次数比等；(2)生成变量重组方案的更优算法，使之能更精确地对变量进行分组，并且可以用于支持更多的数据重组(如结构拆分、结构属性域位置调整等)；(3)在数据重组框架上实现了结构拆分，并进行了更多的实验。

**结束语** 本文介绍了一种基于局部性的数据重组框架，该框架中基于表示变量时间局部性的复用距离的分布特征，设计了一种变量关系图来量化变量之间的关系，在此基础上寻找变量的优化布局，利用数组重组和结构拆分两种数据重组方法来优化程序的 Cache 性能，从而提高整个程序的性能。针对来自 SPEC CPU2000 的部分测试程序的实验表明，这种数据重组框架能够有效地改善程序的数据 Cache 性能，从而提高整个程序的性能。

我们未来的工作主要包含两部分：一是在此基础上实现更多的数据重组方法，如结构属性域位置调整、全局数据和堆数据的交换等；二是将数据重组方法用于包括 GCC 在内的产品编译器，提高编译器的优化效率。

## 参 考 文 献


[1] Patterson D, Anderson T, Cardwell N, et al. A Case for Intelligent RAM. IEEE Micro, 1997: 34-44

[2] Beyls K. Software Methods to Improve Data Locality and Cache Behavior. PhD thesis. Ghent University, 2004

[3] McKinley K S, Carr S, Tseng C W. Improving Data Locality with Loop Transformations. ACM Transactions on Programming Languages and Systems, 1996, 18(4): 424-453

[4] Wu Youfeng. Efficient Discovery of Regular Stride Patterns in Irregular Programs and Its Use in Compiler Prefetching // Proceedings of PLDI'02. June 2002: 210-221

[5] Calder B, Krintz C, John S, et al. Cache-conscious data placement // Proceedings of ASPLOS'98. San Jose, October, 1998: 139-149

[6] Chilimbi T M, Davidson B, Larus J R. Cache-conscious Structure Definition // Proceedings of PLDI'99. May 1999: 13-24

[7] Berg E, Hagersten E. StatCache: A Probabilistic Approach to Efficient and Accurate Data Locality Analysis // Proceedings of ISPASS'04. March 2004: 20-27

[8] Zhong Y, Orlovich M, Shen X, et al. Array regrouping and structure splitting using whole-program reference affinity // Proceedings of PLDI'04. June 2004: 255-266

[9] Hagog M, Tice C. Cache Aware Data Layout Reorganization Optimization in GCC // Proceedings of the GCC Developers' Summit. June 2005: 69-92

[10] Fu Xiong, Zhang Yu, Chen Yiyun. Data-layout Optimization Using Reuse Distance Distribution // The Proceedings of International Workshop on Embedded Software Optimization (ESO'06). Vol. 4097 of Lecture Notes in Computer Science. Seoul, Korea, August 2006: 858-867

[11] McIntosh N, Mannarswamy S, Hundt R. Whole-Program Optimization of Global Variable Layout // Proceedings of PACT'06. Washington, DC, September 2006

[12] Wilson B P, et al. SUIF: A Parallelizing and Optimizing Research Compiler. ACM SIGPLAN Notices, 1994, 29(12): 31-37

[13] Steensgaard B. Points-to Analysis in Almost Linear Time // Proceedings of POPL'96. St. Petersburg, Jan. 1996

[14] Luk Chi-Keung, Cohn R, et al. Pin: Building Customized Program Analysis Tools with Dynamic Instrumentation // Proceedings of PLDI'05. Chicago, Illinois, USA, June 2005: 190-200

[15] Sugumar R A, Abraham S G. Efficient simulation of multiple cache configurations using binomial trees. Technical Report CSE-TR-111-91. University of Michigan, 1991


(上接第 131 页)

## 参 考 文 献


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

[2] Kailar R. Accountability in electronic commerce protocols[J]. IEEE Transactions on Software Engineering, 1996, 22(5): 313-328

[3] Abadi M, Gordon D. A calculus for cryptographic protocols: The spi calculus[C] // Proceedings of the Fourth ACM Conference on Computer and Communications Security. 1997

[4] Abadi M, Gordon D. Reasoning about cryptographic protocols in the spi calculus[C]. Technical Report 414. University of Cambridge Computer Laboratory, 1997

[5] Lowe G. Breaking and fixing the Needham-Schroeder public-key protocol using FDR[C] // Tools and Algorithms for the Construction and Analysis of Systems, volume 1055 of Lecture Notes in Computer Science. Springer-Verlag, 1996: 147-166

[6] Fabrega F, Herzog J, Guttman J. Strand space: why is a security protocol correct [C] // Proceedings of the 1998 IEEE Symposium on Security and Privacy. California, USA: IEEE Computer Society Press, 1998: 160-171

[7] Fabrega F, Herzog J, Guttman J. Honest ideals on strand space [C] // Proceedings of the IEEE Computer Security Foundations Workshop XI. California, USA: IEEE Computer Society Press, 1998: 66-77

[8] 刘璟，祝世雄，周明天. Yahalom 协议的串空间模型及分析[J]. 小型微型计算机系统，2006，05：788-792

[9] Furqan Z, Muhammad S, Guha R. Formal Verification of 802.11i using Strand Space Formalism [C] // Proceedings of the International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies. California, USA: IEEE Computer Society Press, 2006

[10] Miloslavskaya M, Tolstoy A, Ushakov D. Protocol of Secure Mutual Authentication [C] // Proceedings of the 2007 IEEE Workshop on Information Assurance. IEEE SMC, 2007: 43-48

[11] Li Yongjian, Pang Jun. Generalized Unsolicited Tests for Authentication Protocol Analysis [C] // Proceedings of the Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies. California, USA: IEEE Computer Society Press, 2006: 509-514