文章编号:0253-2778(2010)01-0098-05

对 Yahalom-Paulson 协议的分析与改进

陆 超,周 颢,赵保华

(中国科学技术大学计算机科学技术系,安徽合肥 230027)

摘要:对原始 Yahalom-Paulson 协议和 Backes 与 Pfitzmann 的简化 Yahalom-Paulson 协议进行分析,指出各自协议中存在的漏洞.原始协议中存在类型缺陷攻击,简化协议中存在重放攻击导致协议参与实体间会话密钥不一致.对 Yahalom-Paulson 协议作出改进并使用串空间理论证明改进后协议的正确性.

关键词:Yahalom-Paulson 协议;类型缺陷攻击;串空间

中图分类号:TP309 **文献标识码**:A doi:10.3969/j.issn.0253-2778.2010.01.017

Analysis of Yahalom-Paulson protocol and its improvement

LU Chao, ZHOU Hao, ZHAO Baohua

(*Department of Computer and Technology, University of Science and Technology of China, Hefei* 230027, *China*)

Abstract: A detailed analysis of the original Yahalom-Paulson protocol and its simplified version given by Backes and Pfitzmann was presented. It was found that there exists a type flaw attack on the original one and the simplified one can not guarantee the agreement on new session keys between legitimate parties due to replay attacks. The protocol was adapted and the new version was proved correct based on strand space theory.

Key words: Yahalom-Paulson protocol; type flaw attack; strand space

0 引言

Yahalom 协议最初是由 Burrows 等人在他们的经典论文[1]给出的.该协议有三个参与实体:发起者、响应者和可信服务器,使用对称密钥加密,通过四条消息交互完成发起者与响应者之间的相互认证以及由可信服务器生成的会话密钥分发.Yahalom 协议虽然交互简单,但由于其消息结构内在的巧妙,是目前使用形式方法分析最为复杂的协议之一[2].在文献[1]中,Burrows 等人使用 BAN 逻辑对 Yahalom 协议进行分析,指出在协议运行过程中若存在恶意参与实体,则存在对协议的重放攻击.Burrows 将该协议改进为 BAN-Yahalom 协议,同样采用 BAN 逻辑分析并证明了 BAN-Yahalom 协议的安全性.Syverson 在文献[3]中给出了对 BAN-Yahalom 协议的两种攻击方式:第一种说明该协议存在类型缺陷攻击[4],第二种说明该协议存在攻击者的冒充,无法完成协议正常发起者与响应者之间的认证.Paulson 在文献[2]中对 Yahalom 协议修改,给出了 Yahalom-Paulson 协议,运用归纳推理方法并结合通用定理证明器 Isabelle 证明了修改后协议的安全性.Backes 和 Pfitzmann 在文献[5]中认为

收稿日期:2008-03-28;**修回日期**:2008-09-02

基金项目:国家自然科学基金重大研究计划(90104010),国家自然科学基金(60241004)和国家重点基础研究发展(973)计划(2003CB314801)资助.

作者简介:陆超,男,1981 年生,博士生. 研究方向:安全系统验证、协议理论与工程. E-mail:luchao@mail.ustc.edu.cn

通讯作者:周颢,讲师. E-mail:kitewind@ustc.edu.cn

Yahalom-Paulson 协议从可计算模型上不满足密钥保密性并对该协议简单修改，并基于加密库(crytographic library)证明了修改后协议满足密钥保密性. 其他一些学者像 Lowe 也对原始 Yahalom 协议进行修改[6](交互消息数增至 5 条)并使用模型检测的方法证明修改后的协议不存在任何形式的攻击.

我们对 Yahalom-Paulson 协议进行了详细分析，首先指出 Backes 和 Pfitzmann 给出的简化 Yahalom-Paulson 协议存在漏洞，其次指出 Yahalom-Paulson 协议存在类型缺陷攻击，然后对 Yahalom-Paulson 进行改进，改进后的协议不仅满足 Backes 和 Pfitzmann 所提出的密钥保密性，而且能抵御类型缺陷攻击，最后使用串空间理论[7-9]证明改进后协议的正确性.

1　Yahalom-Paulson 协议

Yahalom-Paulson 协议是由 Paulson 在文献[2]中给出的. 该协议整体框架(图 1)与原始 Yahalom 协议一致，共三个参与实体：协议发起者、协议响应者和可信第三方(third trust party, TTP)服务器. 协议使用对称密钥加密，完成协议发起者与响应者之间的相互认证以及会话密钥(由可信服务器生成)的秘密分发. 整个协议一共四条消息交互，规范描述如下：

(Ⅰ)$A\rightarrow B: A, N_a$

(Ⅱ)$B\rightarrow S: B, N_b, \{A, N_a\}_{K_{bs}}$

(Ⅲ)$S\rightarrow A: N_b, \{B, K, N_a\}_{K_{as}}, \{A, B, K, N_b\}_{K_{bs}}$

(Ⅳ)$A\rightarrow B: \{A, B, K, N_b\}_{K_{bs}}, \{N_b\}_K$

其中，A，B 及 S 分别表协议发起者、响应者和服务器；N_a，N_b 分别是 A 和 B 各自产生的随机数；K_{as}，K_{bs} 对应为 A、B 和 S 的对称私有密钥；K 是服务器分发的会话密钥.

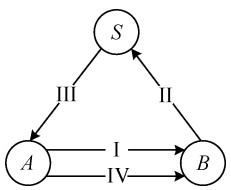

图 1　Yahalom-Paulson 协议

Fig. 1　Yahalom-Paulson protocol

2　协议分析与改进

2.1　Backes 和 Pfitzmann 的简化 Yahalom-Paulson 协议

在文献[5]中，Backes 和 Pfifzmann 认为：从密码学的角度，一个密钥是保密的当且仅当该密钥和一个随机选取的密钥对攻击者来说从计算上不可区分. 他们指出 Yahalom-Paulson 协议不满足该保密性，原因简单描述如下：

在 Yahalom-Paulson 协议一轮正常运行过程中，攻击者截取消息(Ⅱ)和消息(Ⅳ)从而获得 N_b 和 $\{N_b\}_K$，攻击者随机选取密钥 K' 并对 $\{N_b\}_K$ 解密得到 N'_b，通过判断 N_b 是否与 N'_b 相等从而从计算上可以区分 K 与 K'.

Backes 和 Pfifzmann 简单的将 $\{N_b\}_K$ 从消息(Ⅳ)中去掉，并使用加密库的方法证明了修改后的协议满足可计算上的密钥保密性.

我们使用串空间理论对简化协议进行了分析，发现该简化协议存在重放攻击，最终导致协议发起者和响应者最终获得的会话密钥不一致. 攻击过程如下：

(Ⅰ)$A\rightarrow B: A, N_a$

(Ⅱ)$B\rightarrow I(S): B, N_b, \{A, N_a\}_{K_{bs}}$

(Ⅱ′)$I(B)\rightarrow S: B, N_b, \{A, N_a\}_{K_{bs}}$

(Ⅲ′)$S\rightarrow I(A): N_b, \{B, K, N_a\}_{K_{as}}, \{A, B, K, N_b\}_{K_{bs}}$

(Ⅱ″)$I(B)\rightarrow S: B, N_b, \{A, N_a\}_{K_{bs}}$

(Ⅲ″)$S\rightarrow I(A): N_b, \{B, K', N_a\}_{K_{as}}, \{A, B, K', N_b\}_{K_{bs}}$

(Ⅲ)$I(S)\rightarrow A: N_b, \{B, K, N_a\}_{K_{as}}, \{A, B, K', N_b\}_{K_{bs}}$

(Ⅳ)$A\rightarrow B: \{A, B, K', N_b\}_{K_{bs}}$

其中，I 表示攻击者；$I(X)$表示 I 冒充 X.

在该攻击过程中，攻击者截取消息(Ⅱ)并重放此消息，相应地服务器 S 发送消息(Ⅲ′)和消息(Ⅲ″)，其中一个含会话密钥 K，另一个为 K'. 攻击者截取消息(Ⅲ′)和(Ⅲ″)，将(Ⅲ′)的第一个加密项与(Ⅲ″)的第二个加密项相连接构造出消息(Ⅲ)发送给 A，最终导致 A 拥有会话密钥 K，而 B 拥有的会话密钥是 K'.

2.2　对 Yahalom-Paulson 协议的类型缺陷攻击

假设 Yahalom-Paulson 协议运行时不对消息(Ⅰ)的长度做检查，我们发现该协议存在类型缺陷攻击，攻击者可以成功地冒充协议发起者和协议响应者.

2.2.1　攻击者冒充协议发起者

(Ⅰ)$I(A)\rightarrow B: A, N_a$

(Ⅱ)$B\rightarrow I(S): B, N_b, \{A, N_a\}_{K_{bs}}$

(Ⅰ′)$I(A)\rightarrow B: A, B, K, N_b$

(Ⅱ′) $B\rightarrow I(S): B, N'_b, \{A, B, K, N_b\}_{K_{bs}}$

(Ⅲ)跳过

(Ⅳ)$I(A)\rightarrow B:\{A,B,K,N_b\}_{K_{bs}},\{N_b\}_K$

攻击者成功冒充成 A,并与 B 拥有攻击者构造的会话密钥 K.

2.2.2 攻击者冒充协议响应者

(Ⅰ)$A\rightarrow I(B):A,N_a$

(Ⅰ′)$I(B)\rightarrow A:B,K,N_a$

(Ⅱ′)$A\rightarrow I(S):A,N'_a,\{B,K,N_a\}_{K_{as}}$

(Ⅱ)跳过

(Ⅲ)$I(S)\rightarrow A:N_b,\{B,K,N_a\}_{K_{as}},H$

(Ⅳ)$A\rightarrow I(B):H,\{N_b\}_K$

其中 H 为任意加密消息项. 攻击者成功冒充成 B,并与 A 拥有攻击者构造的会话密钥 K.

2.3 对 Yahalom-Paulson 协议的改进

由 2.1 节中对 Backes 和 Pfifzmann 的简化 Yahalom-Paulson 协议的攻击,可以发现 $\{N_b\}_K$ 不能简单的从消息(Ⅳ)中去除,协议响应者通过该项验证他与协议发起者之间的新会话密钥是否一致. 在 Yahalom-Paulson 协议运行过程中,由于攻击者能同时获取 N_b 与 $\{N_b\}_K$ 两项,导致 Yahalom-Paulson 协议不满足 Backes 和 Pfifzmann 所提出的可计算上的密钥保密性. 为此本文对 Yahalom-Paulson 协议的改进将保留 $\{N_b\}_K$ 项,并将 N_b 置入加密项中以保证其秘密性,这样改进后攻击者无法同时获取 N_b 与 $\{N_b\}_K$ 两项,从而满足可计算上的密钥保密性. 在下文中我们将使用串空间理论证明改进后协议中 N_b 的保密性.

2.2 节中对 Yahalom-Paulson 协议的类型缺陷攻击主要是由于该协议中各个加密项结构一致而导致的. 以攻击者冒充协议发起者为例,攻击者为了构造出消息(Ⅳ)中的第一个加密项,可利用的有消息(Ⅱ)中的加密项和消息(Ⅲ)中的第一个加密项. 由于消息(Ⅲ)第一个加密项中协议参与实体标识后紧跟着会话密钥,因此不能用来构造. 如 2.2 节中攻击者成功利用消息(Ⅱ)构造出消息(Ⅳ),从而成功冒充为协议发起者. 为此,本文通过修改协议消息中加密项来破坏原有的结构一致性.

综上,改进后的 Yahalom-Paulson 协议规范如下:

(Ⅰ)$A\rightarrow B:A,N_a$

(Ⅱ)$B\rightarrow S:B,\{A,N_a,N_b\}_{K_{bs}}$

(Ⅲ)$S\rightarrow A:\{N_a,N_b,K,B\}_{K_{as}},\{N_b,K\}_{K_{bs}}$

(Ⅳ)$A\rightarrow B:\{N_b,K\}_{K_{bs}},\{N_b\}_K$

改进后的协议能抵御如 2.2 节中的类型缺陷攻击. 以攻击者冒充协议响应者 B 为例,为了欺骗协议响应者 A,攻击者必须构造出消息(Ⅲ)中的第一个加密项 $\{N_a,N_b,K,B\}_{K_{as}}$,能利用的只有消息(Ⅱ)中的加密项 $\{X,N_x,N_y\}_{K_{ys}}$. 但 $\{N_a,N_b,K,B\}_{K_{as}}$ 中以协议标识结尾,$\{X,N_x,N_y\}_{K_{ys}}$ 以随机数结尾,两者不相交,所以攻击者无法构造出消息(Ⅲ)中的第一个加密项,成功抵御了类型缺陷攻击. 对于攻击者冒充协议发起者的情况,分析类似.

改进后的协议能完成 Yahalom-Paulson 的设计目标,即协议发起者和响应者之间能够相互认证,服务器生成新的会话密钥分发给协议发起者和响应者,能够保证发起者和响应者之间新会话密钥的一致性与保密性. 另外在改进的协议中 N_b 始终是保密的,从而能够满足 Backes 和 Pfifzmann 所提出的可计算上的密钥保密性. 下文使用串空间理论证明改进后协议的认证性,密钥的一致性、保密性和 N_b 的保密性.

3 协议正确性证明

本节使用串空间理论[7-9]证明改进后协议的正确性,为清楚描述协议的串空间模型,作如下定义及记号约定:

(Ⅰ)T_{name} 表示协议参与实体标识集合,是 T 的子集,A、$B\in T_{\text{name}}$;

(Ⅱ)单射函数 $\text{SK}:T_{\text{name}}\rightarrow K$,将协议实体映射至该实体与服务器之间的私有密钥,记 $\text{SK}(A)=K_{as}$,$K_{as}=K_{as}^{-1}$,表示 K_{as} 是对称密钥.

图 2 是协议的串空间图表示.

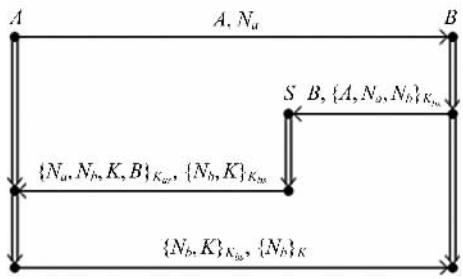

图 2 改进后的 Yahalom-Paulson 协议中的消息交换

Fig. 2 Message exchange in adapted Yahalom-Paulson protocol

3.1 改进后 Yahalom-Paulson 协议的串空间模型

定义 3.1 (Ⅰ)发起者串集合 $\text{Init}[A,B,N_a,N_b,K,H]$,集合中元素的迹为

$$\left.\begin{array}{l}\langle +AN_a,-\{N_aN_bKB\}_{K_{as}}H,+H\{N_b\}_K\rangle,\\ A,B\in T_{\text{name}},N_a\notin T_{\text{name}};\end{array}\right\}$$

(Ⅱ)响应者串集合 Resp$[A,B,N_a,N_b,K]$,集合中元素的迹为

$$\left.\begin{array}{l}\langle -AN_a,+B\{AN_aN_b\}_{K_{bs}}-\{N_bK\}_{K_{bs}}\{N_b\}_K\rangle,\\ A,B\in T_{\text{name}},N_b\notin T_{\text{name}},N_a\neq N_b;\end{array}\right\}$$

(Ⅲ)服务器串集合 Serv$[A,B,N_a,N_b,K]$,集合中元素的迹为

$$\left.\begin{array}{l}\langle -B\{AN_aN_b\}_{K_{bs}},+\{N_aN_bKB\}_{K_{as}}\{N_bK\}_{K_{bs}}\rangle,\\ K\notin K_P,K\notin\{K_{as}:A\in T_{\text{name}}\},K=K^{-1}.\end{array}\right\}$$

定义 3.2　改进的 Yahalom-Paulson 协议串空间 $\Sigma=\text{Serv}\cup\text{Init}\cup\text{Resp}\cup P$,其中 P 为攻击者串集合.

下面在一固定的 Σ 上证明协议的正确性.

3.2　新会话密钥 K 的保密性

定理 3.3　设 C 是 Σ 上的一个束,$s_{\text{serv}}\in\text{Serv}[A,B,N_a,N_b,K]$,$A,B\in T_{\text{name}}$,$K$ 唯一源于 C. 令 $S=\{K,K_{as},K_{bs}\}$,$k=K\setminus S$,$S\cap K_P=\varnothing$. 则 $\forall n\in C.\ \text{term}(n)\notin I_k[K]$.

证明　由文献[9]中的定理 6.3,只需证明 $\forall n\in C.\ \text{term}(n)\notin I_k[S]$. 又由文献[9]中的定理 6.12,只需证明任何正常者串结点 $n\in C$ 不是 $I_k[S]$的入点. 假设存在,由入点定义可知:$\text{term}(n)\in I_k[S]$且 $\text{sign}(n)=+$. 根据文献[9]中的定理 6.3,S 中必有一元素是 $\text{term}(n)$的子项. 又任意正常者串结点不含形如 $K_{xs}(X\in T_{\text{name}})$的子项,故 $K\subset\text{term}(n)$. 逐一检查正常者串结点存在两种情况:

(Ⅰ)$\exists s\in\text{Init},n=\langle s,3\rangle$且 $K\subset H$;

(Ⅱ)$\exists s\in\text{Serv},n=\langle s,2\rangle$且 K 是 s 生成的会话密钥.

对于情况(Ⅰ),$H\subset\langle s,2\rangle$且 $\text{sign}(\langle s,2\rangle)=-$,与 n 是入点矛盾;

对于情况(Ⅱ),因为 K 唯一源于 C,所以 $s=s_{\text{serv}}$,则 $\text{term}(n)=+\{N_aN_bKB\}_{K_{as}}\{N_bK\}_{K_{bs}}$. 根据文献[9]中的定理 6.8 得:$\{N_aN_bKB\}_{K_{as}}\in I_k[S]$或 $\{N_bK\}_{K_{bs}}\in I_k[S]$,则由文献[9]中的定理 6.7 得:$K_{as}\in k$ 或 $K_{bs}\in k$,与 $S\cap K_P=\varnothing$ 矛盾. 故假设有误,即任何正常者串结点$n\in C$不是 $I_k[S]$的入点,由文献[9]中的定理 6.12 立得 $\forall n\in C.\ \text{term}(n)\notin I_k[K]$. 证毕.

3.3　N_b 的保密性

定理 3.4　设 C 是 Σ 上的一个束,$s_{\text{resp}}\in\text{Resp}[A,B,N_a,N_b,K]$,$A,B\in T_{\text{name}}$,$N_b$ 唯一源于 C,$N_a\neq N_b$. 令 $S=\{K,K_{as},K_{bs},N_b\}$,$k=K\setminus S$,$S\cap K_P=\varnothing$. 则 $\forall n\in C.\ \text{term}(n)\notin I_k[N_b]$.

证明　同定理 3.3 证明方法.

3.4　协议的认证性

引理 3.5　设 C 是 Σ 上的一个束,N 唯一源于 C,若 N 是保密的,则 $\{N\}_K$ 不可能源于攻击者结点.

证明　假设 $\{N\}_K$ 源于 C 中的攻击者结点,逐个考虑各种攻击者串. M、F、T、C、S、K 及 D 串型均不可能,考虑 $E.\langle -K,-h,+\{h\}_K\rangle$,则 $\{N\}_K$ 源于 $+\{h\}_K$ 且 $N=h$,这与 N 是保密的相矛盾. 所以该引理成立.

引理 3.6　C 是 Σ 上的一个束,设 $K_{xs}\notin K_P$,其中 $X\in T_{\text{name}}$. 则所有形如 $\{g\}_{K_{xs}}$ 的项不可能源于攻击者结点.

证明　同引理 3.5.

引理 3.7　设 s 是 Σ 上的一个正常者串:

(Ⅰ)如果 $\{XN_1N_2\}_{K_{ys}}$ 源于 s 且 $N_1\neq N_2$,则 $s\in\bigcup_K\text{Resp}[X,Y,N_1,N_2,K]$ 且 $\{XN_1N_2\}_{K_{ys}}$ 源于 $\langle s,2\rangle$、N_2 源于 s;

(Ⅱ)如果 $\{N_1N_2KY\}_{K_{xs}}$ 源于 s 且 $X,Y\in T_{\text{name}}$,$X\neq Y$,则 $s\in\text{Serv}[X,Y,N_1,N_2,K]$ 且 $\{N_1N_2KY\}_{K_{xs}}$ 源于$\langle s,2\rangle$、K 源于 s;

(Ⅲ)如果 $\{N_2K\}_{K_{ys}}$ 源于 s 且 $X\in T_{\text{name}}$,则 $S\in\bigcup_{X,N_1}\text{Serv}[X,Y,N_1,N_2,K]$且 $\{N_2K\}_{K_{ys}}$ 源于$\langle s,2\rangle$、K 源于 s;

(Ⅳ)如果 $\{N_2\}_K$ 源于 s,则 $s_{\bigcup_{X,Y,N_1,H}\text{Init}[X,Y,N_1,N_2,K,H]}$且 $\{N_2\}_K$ 源于$\langle s,3\rangle$.

证明　由所给项形式逐一检查正常者串结点,易证.

3.4.1　协议响应者认证

定理 3.8　C 是 Σ 上的一个束,若 C 中有 $s_{\text{resp}}\in\text{Resp}[A,B,N_a,N_b,K]$ 且 $\text{height}_C(s_{\text{resp}})=3$,其中 $A,B\in T_{\text{name}}$,$A\neq B$,$K_{as},K_{bs},K\notin K_P$,$N_b$、$K$ 唯一源于 C,$N_b\neq N_a$,则 C 中一定有:

(Ⅰ)$s_{\text{serv}}\in\text{Serv}[A,B,N_a,N_b,K]$ 且 $\text{height}_C(s_{\text{serv}})=2$;

(Ⅱ)$s_{\text{init}}\in\text{Init}[A,B,N_a,N_b,K,H]$ 且 $\text{height}_C(s_{\text{init}})=3$.

证明　由假设可知 s_{resp} 的迹为:$\langle -AN_a,+B\{AN_aN_b\}_{K_{bs}},-\{N_bK\}_{K_{bs}}\{N_b\}_K\rangle$,$N_b$ 唯一源于 $\langle s_{\text{resp}},2\rangle$.

(Ⅰ)由引理 3.6 和 3.7 可知$\{N_bK\}_{K_{bs}}$ 源于 $s_{\text{serv}}\in$

$\mathrm{Serv}[X,B,N,N_b,K]$且$\{N_bK\}_{K_{bs}}$源于$\langle s_{\mathrm{serv}},2\rangle$、$K$源于$s_{\mathrm{serv}}$.

考虑$\langle s_{\mathrm{serv}},1\rangle$的子项$\{XNN_b\}_{K_{bs}}$,由引理 3.6 和 3.7 可知该项源于 $s_1\in\mathrm{Resp}[X,B,N,N_b,K']$,则 N_b 源于$\langle s_1,2\rangle$. 由 N_b 的唯一性可得:$s_1=s_{\mathrm{resp}}$,则 $X=A,N=N_a,K'=K$,所以 $s_{\mathrm{serv}}\in\mathrm{Serv}[A,B,N_a,N_b,K]$. 又$\langle s_{\mathrm{serv}},2\rangle\in C$,所以 $\mathrm{height}_C(s_{\mathrm{serv}})=2$.

(Ⅱ)由引理 3.6 和 3.7 可知$\{N_b\}_K$ 源于 $s_{\mathrm{init}}\in\mathrm{Init}[X,Y,N,N_b,K,H]$且$\{N_b\}_K$ 源于$\langle s_{\mathrm{init}},3\rangle$. 考虑$\langle s_{\mathrm{init}},2\rangle$的子项$\{NN_bKY\}_{K_{xs}}$,由引理 3.6 和 3.7 可知该项源于 $s_2\in\mathrm{Serv}[X,Y,N,N_b,K]$且$\{NN_bKY]_{K_{xs}}$源于$\langle s_2,2\rangle$、$K$ 源于 s_2. 由证明(Ⅰ)知 K 源于 s_{serv},K 又唯一源于 C,所以 $s_2=s_{\mathrm{serv}}$,则:$X=A,Y=B,N=N_a$. 所以 $s_{\mathrm{init}}\in\mathrm{Init}[A,B,N_a,N_b,K,H]$,又$\langle s_{\mathrm{init}},3\rangle\in C$,故 $\mathrm{height}_C(s_{\mathrm{init}})=3$.

综上,定理 3.8 得证.

3.4.2 协议发起者认证

定理 3.9 C 是Σ上的一个束,若 C 中有 $s_{\mathrm{init}}\in\mathrm{Init}[A,B,N_a,N_b,K,H]$且 $\mathrm{height}_C(s_{\mathrm{init}})=3$,其中 $A,B\in T_{\mathrm{name}},A\neq B,K_{as},K_{bs},K\notin K_P,N_a$、$K$ 唯一源于 C,则 C 中一定有

(Ⅰ) $s_{\mathrm{serv}}\in\mathrm{Serv}[A,B,N_a,N_b,K]$且 $\mathrm{height}_C(s_{\mathrm{serv}})=2$;

(Ⅱ) $s_{\mathrm{resp}}\in\mathrm{Resp}[A,B,N_a,N_b,*]$且 $\mathrm{height}_C(s_{\mathrm{resp}})\geqslant 2$.

证明 类似定理 3.8 的证明.

综上,由定理 3.3、3.8 和 3.9 可知改进后的 Yahalom-Paulson 协议的正确性.

4 结论

本文对 Yahalom-Paulson 协议进行详细分析,包括原始的 Yahalom-Paulson 协议和 Backes 和 Pfifzmann 的简化 Yahalom-Paulson 协议,指出了这两个协议存在的漏洞. 原始 Yahalom-Paulson 协议存在类型缺陷攻击,简化 Yahalom-Paulson 协议存在重放攻击导致协议正常参与实体间无法达成会话密钥一致. 为此本文给出了改进的 Yahalom-Paulson 协议,改进后的协议不仅能抵御上述几种攻击,而且能完成协议设计的原始目标:包括协议参与实体间的认证、会话密钥的保密与一致. 另外改进后的协议还满足 Backes 和 Pfifzmann 提出的计算上的密钥保密性. 最后本文利用串空间理论证明了改进后协议的正确性.

参考文献(References)

[1] Burrows M, Abadi M, Needham R M. A logic of authentication[J]. Proceedings of the Royal Society of London, 1989, 426: 223-271.

[2] Paulson L C. Relations between secrets: Two formal analyses of the Yahalom protocol[J]. Journal of Computer Security, 2001, 9(3): 197-216.

[3] Paul Syverson. A taxonomy of replay attacks[C]// Proceedings of the Computer Security Foundations Workshop(CSFW 7), 1994: 187-191.

[4] Carlsen U. Cryptographic protocol flaws: Know your enemy[C]//Proceeding s of the Computer Security Foundations Workshop(CSFW 7), 1994: 192-200.

[5] Michael Backes, Birgit Pfitzmann. On the cryptographic key secrecy of the strengthened Yahalom protocol[C]//Proceedings of 21st IFIP International Information Security Conference (SEC), 2006: 233-245.

[6] Gavin Lowe. Towards a completeness result for model checking of security protocols[J]. Journal of Computer Security, 1999, 7(2-3): 89-146.

[7] Fábrega F T, Herzog J, Guttman J. Strand spaces: Why is a security protocol correct? [C]//Proceedings of 1998 IEEE Symposium on Security and Privacy, 1998: 160-171.

[8] Fábrega F T, Herzog J, Guttman J. Honest ideals on strand spaces[C]//Proceedings of the 11th IEEE Computer Security Foundations Workshop, 1998: 66-77.

[9] Fábrega F T, Herzog J, Guttman J. Strand spaces: Proving security protocols correct[J]. Journal of Computer Security, 1999, 7(2-3): 191-230.