ISSN 1000-9825 Journal of Software 软件学报 2000,11(10):1338~1343

一种新型的非否认协议*

卿斯汉

(中国科学院软件研究所信息安全国家重点实验室 北京 100080)
(中国科学院信息安全技术工程研究中心 北京 100080)
E-mail: qsihan@yahoo.com

摘要 在克服一种非否认协议草案的缺陷的基础上,提出一种新的非否认协议.新的协议可以在不安全和不可靠的信道上工作,并能对付各种欺骗行为.此外,还对SVO逻辑进行扩充,引进一些新的概念和方法,并用扩展后的SVO逻辑分析与证明新的非否认协议.

关键词 非否认协议,SVO逻辑,可信第三方,仲裁方.
中图法分类号 TP309

ISO曾经制定若干关于非否认协议的标准草案[1~3].在文献[2]中,提出了4种不同的非否认协议,我们只讨论其中的一个,即协议M2.本文首先指出,这个利用对称密码算法的协议在防止欺骗方面存在缺陷.然后,我们提出一种新的非否认协议,并用扩展的SVO逻辑[4]证明其正确性.最后,我们将在结论中总结本文提出的一些新的概念和方法.

1 概念与符号

1.1 概 念

(1) 非否认协议的目标:收集、保存、使用和证实各种无可辨驳的证据.

(2) 非否认协议执行的不同阶段:①证据生成;②证据传输、存储与提取;③证据校验;④争议仲裁.

(3) 仲裁方(adjudicator,简称ADJ):可以根据证据解决争议的实体.

(4) POO(proof of origin)标志:使接收方可以建立报文来源证明的数据项.

(5) POR(proof fo receipt)标志:使发送方可以建立报文接收证明的数据项.

(6) 安全封装SENV(secure envelope):数据项的具有特殊构造的集合,使接收方可以验证其来源与完整性.

(7) 可信第三方TTP(trusted third party):在执行协议的过程中,发送方、接收方和仲裁方都信任的实体.

1.2 符 号

a是仅由实体A和TTP共享的密钥;b是仅由实体B和TTP共享的密钥;x是TTP独享的密钥;M是由实体A发送给实体B的报文;(X,Y)是数据项X和Y按此顺序的连接;K_{ab}是实体A和实体B之间的会话密钥;$\{X\}_K$是用密钥K加密数据X后的密文;$h(X)$是数据X的单向杂凑函数;N_a是实体A生成的临时值(nonce);N_b是实体B生成的临时值;N_{ttp}是TTP生成的临时值;N_{adj}是ADJ生成的临时值.

2 ISO非否认协议M2

在协议M2中,报文交换的过程如下:

* 本文研究得到国家重点基础研究发展规划项目(G1999035810)资助.作者卿斯汉,1939年生,研究员,博士生导师,主要研究领域为信息安全理论和技术.

本文通讯联系人:卿斯汉,北京 100080,中国科学院软件研究所

本文2000-05-31收到原稿,2000-06-30收到修改稿

(1) $A\rightarrow$TTP: $\mathrm{SENV}_a(Z)$;

(2) TTP$\rightarrow A$: $\mathrm{SENV}_a(\mathrm{POO})$;

(3) $A\rightarrow B$: M,Z,POO;

(4) $B\rightarrow$TTP: $\mathrm{SENV}_b(\mathrm{POO})$;

(5) TTP$\rightarrow B$: $\mathrm{SENV}_b(\mathrm{PON},\mathrm{POO},\mathrm{POR})$;

(6) TTP$\rightarrow A$: $\mathrm{SENV}_a(\mathrm{POR})$.

其中 Z,Z',POO 与 POR 分别取值如下：

$$Z=\mathrm{POO\ flag},A,B,h(M),$$

$$Z'=\mathrm{POR\ flag},A,B,h(M),$$

$$\mathrm{POO}=\mathrm{keyid},\mathrm{msgid},\mathrm{SENV}_X(Z),$$

$$\mathrm{POR}=\mathrm{keyid},\mathrm{msgid},\mathrm{SENV}_X(Z').$$

此外，PON 是指示对提交给 TTP 的 POO 或 POR 标志的验证结果(真或伪)的数据项.

M2 协议是有缺陷的. 首先，如果 B 在执行协议的第(3)步后停止执行协议，他可以抵赖收到报文 M 这一事实，因为没有任何证据能够证实他的欺骗行为. 其次，在协议的第(3)步，报文 M 是以明文的形式传送的，因此入侵者可以轻易地窃取报文 M. 为此，我们提出一种新的非否认协议，如下文所述.

3 一个新的非否认协议

这个新的非否认协议由下述 6 步构成，其中各符号的含义参看第 4.2.2 节.

(1) $A\rightarrow$TTP: r_{ab},N_a

A 向 TTP 请求启动非否认协议.

(2) TTP$\rightarrow A$: $\mathrm{SENV}_a(i1,N_a,N_{\mathrm{ttp}},K_{ab})$

TTP 通过安全封装向 A 发送会话密钥 K_{ab}.

(3) $A\rightarrow B$: $\{M\}_{K_{ab}},\mathrm{POO}=\mathrm{SENV}_a(r1,N_{\mathrm{ttp}},\{M\}_{K_{ab}})$

A 向 B 发送 POO 及 $\{M\}_{K_{ab}}$. 如果 B 由于某种原因不打算接收报文 M，他可以在此终止协议的运行，而不会引起任何争议.

(4) $B\rightarrow$TTP: $\mathrm{POO},\mathrm{POR}=\mathrm{SENV}_b(r2,N_b,\{M\}_{K_{ab}})$

如果 B 在第(3)步后打算继续执行协议，就将收到的 POO 转发给 TTP，并向 TTP 发送 POR.

(5) TTP$\rightarrow B$: $\mathrm{SENV}_b(i2,N_b,K_{ab})$

如果 TTP 证实 POO 与 POR 的正确性，就通过安全封装向 B 发送 K_{ab}，并通知 B：TTP 相信 A 在协议的本次运行中发送了报文 M. 否则，TTP 中止协议的执行，而不会引起任何争议.

(6) TTP$\rightarrow A$: $\mathrm{SENV}_a(i3,N_a)$

如果 TTP 证实 POO 与 POR 的正确性，就通知 A：TTP 相信 B 收到了报文 M. 否则，TTP 中止协议的执行，而不会引起任何争议.

上述报文序列如图 1 所示.

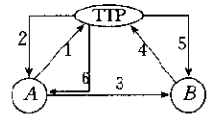

Fig. 1 The new non-repudiation protocol
图1 新的非否认协议示意图

4 用SVO 逻辑分析新的非否认协议

4.1 扩展SVO 逻辑公理

SVO 逻辑继承并发展了 BAN 逻辑[5]，是一种很好的的非否认协议的形式化分析工具. 运用 SVO 逻辑可以发现隐藏在各种密码协议之中的细微的安全缺陷与错误，并提示纠正的途径. 为了分析和证明新的非否认协议，我们为SVO 逻辑增设了以下 4 条公理.

(1) P says $\{X\}_k \wedge P$ has $K \supset P$ says X

对于任意实体 P,如果 P 拥有密钥 K 并发送了用 K 加密 X 后的密文 $\{X\}_K$,则 P 发送了 X.

(2) P says $X \wedge Q$ sees $X \supset Q$ received X

对于任意实体 P 和 Q,如果在协议的本次运行中 P 发送了 X,且 Q 知道 X,那么 Q 必然接收到 X,即 X 不是由 Q 生成的.

(3) $P\_\text{public}\_A(X) \supset P$ believes A sees X

如果实体 P 令实体 A 知道 X,则 P 相信 A 拥有 X.

(4) $\text{public}\_A(X) \supset P$ believes A sees X

如果众所周知实体 A 知道 X,则任意实体 P 都相信 A 拥有 X.

4.2 协议的分析和证明

4.2.1 基本假定

新协议的分析与证明是基于以下假设:

(1) 任意参加协议的实体都相信 TTP 是诚实且胜任的.这一假定可用 SVO 逻辑形式化地表示为

$$P \text{ believes } (((\text{TTP says } X) \wedge (X \supset C)) \supset (\text{TTP believes } C)).$$

(2) 类似地,我们假定任意参加协议的实体都相信 ADJ 是诚实的、胜任的,亦即

$$P \text{ believes } (((\text{ADJ says } X) \wedge (X \supset C)) \supset (\text{ADJ believes } C)).$$

(3) 任意参加协议的实体 A 和 B 都是胜任的,亦即他们各自都明白自己所发送报文的含义.但是,A 和 B 之间是互不信任的.

(4) 任意参加协议的实体都不会故意使自己处于不利的地位,也不会故意使自己成为争议仲裁的输家.

(5) 协议中应用的各种安全保密算法都是完善的,例如,安全封装是真正安全的.

(6) 通信信道既不安全也不可靠,亦即入侵者可能通过信道窃取实体之间交换的报文.此外,通信信道可能出现各种故障.但是,通信信道最终是无故障的,亦即通过各种补救措施和检错纠错等方法,报文在有限时间内可以通过信道正确无误地传输.

4.2.2 初始假设集合

术语集合如下:

$T=\{\{A,B,\text{TTP},\text{ADJ}\},\{a,b,x,K_{ab}\}$,

$\{r_{ab}=$"请求启动非否认协议"标志$\}$,

$r1=$POO 标志,

$r2=$POR 标志,

$i1=$"A 拥有 K_{ab}"标志,

$i2=$"B 拥有 K_{ab}且 A 发送 M"标志,

$i3=$"B 收到 M"标志$\}$.

此处,标志 r_{ab},$r1$ 和 $r2$ 是通常意义下的标志.标志 $i1$,$i2$ 和 $i3$ 用来表示报文的发送者相信该标志所指明的事实.在本文中我们加以限制,只有 TTP 才能在他发送的报文中使用这些标志.

初始公式语言如下:

$$\begin{aligned}
&F_T = \{\\
&A \text{ believes } A \xleftrightarrow{a} \text{TTP}, \text{TTP believes } A \xleftrightarrow{a} \text{TTP},\\
&B \text{ believes } B \xleftrightarrow{b} \text{TTP}, \text{TTP believes } B \xleftrightarrow{a} \text{TTP},\\
&\text{TTP believes } A \xleftrightarrow{K_{ab}} B,\\
&A \text{ believes TTP controls } A \xleftrightarrow{K_{ab}} B,\\
&B \text{ believes TTP controls } A \xleftrightarrow{K_{ab}} B,\\
&\text{TTP believes fresh}(N_{\text{ttp}}),
\end{aligned}$$

A believes fresh(N_a),

B believes fresh(N_b),

A believes A sees (r_{ab},$r1$,$r2$,$i1$,$i2$,$i3$),

B believes B sees (r_{cb},$r1$,$r2$,$i1$,$i2$,$i3$),

A believes TTP controls $i3$,

B believes TTP controls $i2$,

TTP believes TTP sees (r_{ab},$r1$,$r2$),

TTP believes $i1$, TTP believes $i2$,

TTP believes $i3$,}.

4.2.3 理想化后的协议

理想化后的协议如下：

(1) $A\rightarrow$TTP:(r_{ab},N_a);

(2) TTP$\rightarrow A$:SENV$_a$($i1$,N_a,N_{ttp},$A \xleftrightarrow{K_{ab}} B$);

(3) $A\rightarrow B$:($\{M\}_{K_{cb}}$,SENV$_a$($r1$,N_{ttp},$\{M\}_{K_{ab}}$));

(4) $B\rightarrow$TTP:(SENV$_a$($r1$,N_{ttp},$\{M\}_{K_{ab}}$)),SENV$_b$($r2$,N_b,$\{M\}_{K_{ab}}$));

(5) TTP$\rightarrow B$:SENV$_b$($i2$,N_b,$A \xleftrightarrow{K_{ab}} B$);

(6) TTP$\rightarrow A$:SENV$_a$($i3$,N_a).

4.2.4 协议的分析与证明

对于协议的任意一次运行，我们都有：

(1) 报文(1)对协议的逻辑分析没有影响.

(2) 对于报文(2)，我们有

A believes (A received SENV$_a$($i1$,N_a,N_{ttp},$A \xleftrightarrow{K_{ab}} B$) $\wedge$ $A \xleftrightarrow{a}$ TTP)$\supset$

A believes TTP said ($i1$,N_a,N_{ttp},$A \xleftrightarrow{K_{ab}} B$);

A believes (TTP said ($i1$,N_a,N_{ttp},$A \xleftrightarrow{K_{ab}} B$) $\wedge$ fresh(N_a))$\supset$

A believes TTP says $A \xleftrightarrow{K_{ab}} B$;

A believes (TTP says $A \xleftrightarrow{K_{ab}} B \wedge$ TTP controls $A \xleftrightarrow{K_{ab}} B \supset A$ believes $A \xleftrightarrow{K_{ab}} B$;

TTP_public_A($A \xleftrightarrow{K_{cb}} B$)$\supset$TTP believes A sees $A \xleftrightarrow{K_{ab}} B$.

(3) 对于报文(3)，我们有

B believes $\{M\}_{K_{ab}}$;

B believes SENV$_a$($r1$,N_{ttp},$\{M\}_{K_{ab}}$).

(4) 对于报文(4)，我们有

TTP believes (A said ($r1$,N_{ttp},$\{M\}_{K_{ab}} \wedge$ fresh(N_{ttp}))$\supset$TTP believes A says $\{M\}_{K_{ab}}$;

TTP believes (A says $\{M\}_{K_{ab}} \wedge A$ sees $A \xleftrightarrow{K_{ab}} B$)$\supset$TTP believes A says M;

TTP believes (B said ($r2$,N_b,$\{M\}_{K_{ab}}\supset$TTP believes B sees $\{M\}_{K_{ab}}$;

TTP believes (A says $\{M\}_{K_{ab}} \wedge B$ sees $\{M\}_{K_{ab}}$)$\supset$TTP believes B received $\{M\}_{K_{ab}}$.

(5) 对于报文(5)，我们有

B believes (TTP said ($i2$,N_b,$A \xleftrightarrow{K_{ab}} B$) $\wedge$ fresh(N_b))$\supset$

B believes (TTP says $A \xleftrightarrow{K_{ab}} B \wedge$ TTP says $i2$);

B believes (TTP says $A \xleftrightarrow{K_{ab}} B \wedge$ TTP controls $A \xleftrightarrow{K_{ab}} B$)$\supset B$ believes $A \xleftrightarrow{K_{ab}} B$;

B believes (TTP says $i2 \wedge$ TTP controls $i2$)$\supset B$ believes $i2$;

B believes ($i2 \wedge B$ sees $i2$)$\supset B$ believes A says M;

TTP_public_$B(A \overset{K_{ab}}{\longleftrightarrow} B)\supset$TTP believes B sees $A \overset{K_{ab}}{\longleftrightarrow} B$;

TTP believes (B received $\{M\}_{K_{ab}} \wedge B$ sees $A \overset{K_{ab}}{\longleftrightarrow} B)\supset$TTP believes B received M.

(6) 对于报文(6),我们有

A believes TTP said $(i3, N_a) \wedge \mathrm{fresh}(N_a))\supset A$ believes TTP says $i3$;

A believes (TTP says $i3 \wedge$ TTP controls $i3)\supset A$ believes $i3$;

A believes ($i3 \wedge A$ sees $i3)\supset A$ believes B received M.

最后,我们的逻辑分析导致了下述预期的结果:

A believes $A \overset{K_{ab}}{\longleftrightarrow} B$, B believes $A \overset{K_{ab}}{\longleftrightarrow} B$;

A believes B received M, B believes A says M;

TTP believes A says M, TTP believes B received M.

我们注意到 A 相信标志 $i3$ 指示的事实,但是 A 没有证据. A 之所以相信"B 收到 M"是因为当 B 否认收到 A 发送的报文 M 时,A 可以向 TTP 请求提供证据. 类似地,B 也相信标志 $i2$ 指示的事实.

4.3 争议仲裁

在本协议中,我们假定 TTP 同时充当 ADJ 的角色,亦即由 TTP 负责解决 A 和 B 之间的争议.

例如,当 A 否认发送报文 M 时,B 向 ADJ 请求仲裁. 通过使用 POO,ADJ 所执行的仲裁过程如下:

ADJ believes (ADJ received $\mathrm{SENV}_a(r1, N_{ttp}, \{M\}_{K_{ab}} \wedge A \overset{a}{\longleftrightarrow}$ TTP)$\supset$

ADJ believes A said $(r1, N_{ttp}, \{M\}_{K_{ab}})$;

ADJ believes A said $(r1, N_{ttp}, \{M\}_{K_{ab}}) \wedge \mathrm{fresh}(N_{ttp}))\supset$ADJ believes A says $\{M\}_{K_{ab}}$;

ADJ_public_$A(A \overset{K_{ab}}{\longleftrightarrow} B)\supset$ADJ believes A sees $A \overset{K_{ab}}{\longleftrightarrow} B$;

ADJ believes (A says $\{M\}_{K_{ab}} \wedge A$ sees $A \overset{K_{ab}}{\longleftrightarrow} B)\supset$ADJ believes a says M.

当 B 否认收到 A 发送的报文 M 时,A 向 ADJ 请求仲裁. 通过使用 POR,ADJ 进行的仲裁过程是类似的.

5 协议的一个变种

在某些场合下,我们希望 TTP 和 ADJ 是两个不同的角色. 只要对上述协议作少量修改就可以做到. 修改后的协议如下:

(1) $A \rightarrow$TTP: r_{ab}, N_a;

(2) TTP$\rightarrow A$: $\{\text{SIGN-}K_{ttp}(i1, K_{ab}, N_a, N_{ttp})\}_{+K_a}$;

(3) $A \rightarrow B$: POO$=\text{SIGN-}K_a(r1, N_{ttp}, \{M\}_{K_{ab}})$;

(4) $B \rightarrow$TTP: POO, POR$=\text{SIGN-}K_b(r2, N_b, \{M\}_{K_{ab}})$;

(5) TTP$\rightarrow B$: $\{\text{SIGN-}K_{ttp}(i2, K_{ab}, N_b)\}_{+K_b}$;

(6) TTP$\rightarrow A$: $\{\text{SIGN-}K_{ttp}(i1, N_a)\}_{+K_a}$.

上述协议使用了非对称密码算法. 这里,$+K_a$,$+K_b$ 和 $+K_{ttp}$ 分别表示 A,B 和 TTP 拥有的公开密钥. 相应地,$-K_a$,$-K_b$ 和 $-K_{ttp}$ 分别表示 A,B 和 TTP 的与上述公开密钥相匹配的秘密密钥. 符号 SIGN-K_a,SIGN-K_b 和 SIGN-K_{ttp} 分别表示 A,B 和 TTP 的数字签名,其签名密钥分别为 $-K_a$,$-K_b$ 和 $-K_{ttp}$. 关于这种使用混和型密码算法的非否认协议的详细讨论,我们将另文发表.

6 结 论

我们提出的一个新的非否认协议可以运行在不安全和不可靠的信道上,并且能够防止欺骗行为,使协议的各参加方处于一个平等的地位. 为了分析上述协议并证明它的正确性,我们引入了一些新的概念并扩展了 SVO

逻辑公理.(1) 标志 $i1$,$i2$ 和 $i3$ 具有特殊功能,它们不仅像通常的标志那样指示某种特征,而且指示报文发送者所相信的某种事实,从而起了减少通信量的重要作用.(2) 与 ISO 标准草案 M2 协议不同,当协议正常结束时,TTP 只通知 A 和 B 协议本次运行的结果,但不提供任何证据.只有在发生争议必须进行仲裁时,TTP 才生成证据并发送给 ADJ(如果 TTP 与 ADJ 不同).这种方法也减少了通信量.(3) 我们引入了两条特殊的 SVO 逻辑公理,即公理 3 和公理 4,这两条公理的正确性基于"通信信道是最终无故障"的基本假设.(4) 我们发现,两条具有相同格式的报文容易遭受"报文重放"式的攻击[6].因此,在我们的方案中,POO 和 POR 具有不同的格式.

参考文献

1 ISO/IEC/JCT1. 5th Working Draft on Non-Repudiation, Part 1: General Model. ISO/IEC/JCT1/SC27/WG2 N259, 1994

2 ISO/IEC CD 13888-2. Non-Repudiation, Part 2: Using Symmetric Encipherment Algorithms. ISO/IEC/JJC1/SC27 N864, 1994

3 ISO/IEC/JCT1. 3rd Working Draft on Non-Repudiation, Part 3: Using Asymmetric Encipherment Algorithms. ISO/IEC/JTC1/SC27/WG2 N224, 1994

4 Syverson P, Oorschot P van. On unifying some cryptographic protocol logics. In: Proceedings of 1994 IEEE Symposium on Security & Privacy. Oakland, CA: IEEE Computer Society Press, 1994

5 Burrows M, Abadi M, Needham R. A logic of authentication. ACM Transactions on Computer System, 1990,18(1):18~36

6 Qing Si-han. Formal analysis of authentication protocols. Journal of Software, 1996,7(supplement):107~114
(卿斯汉.认证协议的形式化分析.软件学报,1996,7(增刊):107~114)

A New Non-Repudiation Protocol

QING Si-han

(*State Key Laboratory of Information Security Institute of Software The Chinese Academy of Sciences Beijing* 100080)
(*Engineering Research Center for Information Security Technology The Chinese Academy of Sciences Beijing* 100080)

Abstract In this paper, a new non-repudiation protocol is presented based on the correction of an existing protocol which has some security flaws. This scheme can work on an insecure and unreliable communication channel. Besides, it can deal with cheating. Some new notions and approaches for extending the SVO logic are introduced, then the extended SVO logic is used to analyze the new protocol and prove its correctness.

Key words Non Repudiation protocol, SVO logic, trusted third party, adjudicator.