一个非否认协议 ZG 的形式化分析

范 红,冯登国
(中科院研究生院信息安全国家重点实验室,北京 100039)

摘 要: 非否认性是电子商务协议的一个重要性质,其形式化分析问题引起了人们的密切关注. 本文运用 SVO 逻辑对一个非否认协议实例进行了有效的形式化分析,并对协议的缺陷进行了改进.

关键词: 非否认协议; 形式化分析; SVO 逻辑
中图分类号: TN91 **文献标识码**: A **文章编号**: 0372-2112 (2005) 01-0171-03

Formal Analysis of a Non-Repudiation Protocol ZG

FAN Hong, FENG Deng-guo
(State Key Laboratory of Information Security The Chinese Academy of Science, Beijing 100039, China)

Abstract: Non-repudiation is a key property of electronic commerce protocols, and its formal analysis has draw people's attention. This paper analyzes a non-repudiation protocol using formal methods, and modifies some flaws of the protocol.

Key words: non-repudiation protocol; formal analysis; SVO logic

1 引言

近几年,随着电子商务协议的出现,一些新的安全性质及其形式化分析引起人们的密切关注,如协议的非否认性(non-repudiation)[1]. 在认证和密钥分配协议中,主体双方的目标是一致的,如共享一个良好的会话密钥等. 而与之不同的是在有些协议中,主体的目标各不相同,因而主体可根据其各自的目的与利益需求对其已发生行为进行否认. 当出现此类情况时需要非否认技术来解决问题,非否认协议则是非否认技术的一种具体实现,它通过协议设计使得协议主体无法否认其行为,即达成协议的非否认性. 一个协议能否实现非否认性即非否认协议的分析可借助于形式化工具来分析. 形式化分析技术从出现到发展至今已有二十多年的历史,对安全协议的分析起到了非常重要的作用. 本文所运用的推理工具 SVO 逻辑集 BAN 逻辑, GNY 逻辑, AT 逻辑等之大成,吸收了这些逻辑系统的优点[4],并具有十分简洁的推理规则和公理,可用于非否认协议的形式化分析之中,并在此统一框架下可对非否认协议的多种性质进行全面、完整的分析.

2 一个非否认协议实例

非否认协议的出现是由于在电子商务交易中,协议主体具有不同的利益出发点,因此有可能根据其各自需要在事后否认所进行的交易行为,从而给对方造成经济损失,或推卸已方的责任. 非否认协议则试图通过协议的设计杜绝这种可能. 因此,非否认协议必须保证主体在协议的执行过程中的地位是平等的,或者换言之,协议的执行对于主体双方是公平的,而且在协议运行结束时应能够提供有效的证据用以证明主体声称的某一行为的出现或不出现是一个不可反驳的事实. 即保证交易的公平性和证据的有效性. 前者避免了产生否认的客观条件,后者保证一旦出现否认则可通过仲裁依据证据进行裁定加以解决. 非否认协议的实现包括证据的生成,证据的交换,证据的验证以及纠纷的解决,方法一般有两种:一是双方进行同时(或接近同时)的秘密交换[5];另一种是借助一个可信第三方(TTP). 第一种方法实现起来较为麻烦,它要求协议双方具有同等的计算能力,这是不现实的. 因此,往往采用第二种方法. 非否认协议提供的两个基本证据为:NRO(non-repudiation of origin),NRR(non-repudiation of receipt). 如果协议中有可信第三方 TTP 的介入,则还需要下面两个证据:NRS(non-repudiation of submission),NRD(non-repudiation of delivery).

Zhou 和 Collmann 在文献[1]中提出了一个非否认协议(以下称为 ZG 协议),具体描述如下:(1) $A \rightarrow B: fNRO, B, L, C, NRO$; (2) $B \rightarrow A: fNRR, A, L, C, NRR$; (3) $A \rightarrow TTP: fNRS, B, L, K, NRS\_K$; (4) $B \leftrightarrow TTP: fNRD, A, B, L, K, NRD\_K$; (5) $A \leftrightarrow TTP: fNRD, A, B, L, K, NRD\_K$.

其中:A 为非否认协议交换的发起者; B 为非否认协议交换的接收者; TTP 为可提供网络服务的在线可信第三方; M 为 A 发送给 B 的消息; C 为 A 发送给 B 的密文; K 为 A 定义的消息密钥; L 为协议轮的标志; S_I 为表示主体 I 的签名私钥; f_{NRO}, f_{NRR}, f_{NRS} 及 f_{NRD} 为用于标识生成特定消息的协议步骤的标志,为方便起见,简记为 f_1, f_2, f_3 和 f_4; $\leftrightarrow$: ftp 操作符; $NRO = S_A(f_{NRO}, B, L, C)$; $NRR = S_B(f_{NRO}, A, L, C)$; $NRS\_K = S_A(f_{NRS}, B, L, K)$; $NRD\_K = S_{TTP}(f_{NRO}, A, B, L, K)$.

收稿日期:2003-03-20;修回日期:2003-04-20
基金项目:973 资助项目(No. G1999035802);国家杰出青年科学基金(No. 60025205)

3 实例分析

3.1 SVO 逻辑

SVO 逻辑遵从两条推理规则和 20 条公理. 两条规则为:

$I1: \Psi \wedge (\Psi \supset \Phi) \vdash \Phi$ $I2: \vdash \Phi \supset P$ believes Φ

其中 Ψ 和 Φ 是公式, P 表示主体, $\vdash \Phi$ 表示 Φ 是一个可由公理推导而来的公式. 这里仅列出与证明有关的公理.

相信公理 对于任一主体 P 和公式 Ψ, Φ 有:

$P1: P$ believes $\Psi \wedge P$ believes $(\Psi \supset \Phi) \supset P$ believes Φ

$P2: P$ believes $\Psi \supset P$ believes (P believes Ψ)

主体相信由已有的信任关系逻辑推导出的所有信仰结果.

接收公理

$P5: P$ received $(X1, \cdots, Xn) \supset P$ received Xi

$P6: P$ received $\{X\}K \wedge P$ has $K^{-1} \supset P$ received X

主体对接收到的一个级联的加密消息可用有效的密钥解密.

看到公理

$P7: P$ received $X \supset P$ sees X

$P8: P$ sees $(X1, \cdots, Xn)$ P sees Xi

主体只要接收到一个消息就看到了这个消息,并且看到了这个消息的每一部分.

理解公理

$P10: P$ believes $(P$ sees $F(X)) \supset P$ believes $(P$ sees $X)$

$P11: P$ received $F(X) \wedge P$ believes $(P$ sees $X) \supset P$ believes (P received $F(X)$)

如果一个主体理解一个消息,并看到此消息的一个函数,那么它理解它所看到的. F 可视为加解密函数, K 为参数.

叙述公理 $P12: P$ said $(X1, \cdots, Xn) \supset P$ said $Xi \wedge P$ sees Xi

一个主体说过一个级联消息,那么它一定说过且看到消息的每一部分.

3.2 形式化分析

首先,我们提出非否认协议公平性的定义.

定义 3.1 非否认协议的公平性是指从协议执行的开始到协议执行结束的任何一个阶段,通信的双方要么能够同时得到它们所期望的,要么任何一方都得不到有利于自己的信息,从而避免协议的任一方中断执行的协议,或否认其已发生的行为以达成利益不平等的可能.

其次,在定义 3.1 的基础上我们提出下面的定理说明.

定理 3.1 一个非否认协议的非否认性是成立的,如果: (1) 协议任何一步执行后的中止将不会破坏通信双方主体的地位的公平性;并且, (2) 在协议结束时提供主体参与协议行为的有效证据,即证据的有效性. 最后,证明 ZG 协议的非否认性.

证明:

给出协议的前提或假设 $A0$ 基本假设:协议的运行环境是不安全的; $A1$:每个主体的公钥是公开的; $A2$:每个主体的私钥仅为其所知; $A3: TTP$ believes S_A; $A4: TTP$ believes S_B; $A5: P$ believes S_{TTP}; P 为参与协议运行的主体.

$A6: TTP$ believes (B received $C) \supset TTP$ believes (A said $C)$

$A7: A$ said $(A, B, L, Ek(M)) \wedge A$ said (A, B, L, K) A said M; $A8: B$ received $(A, B, L, Ek(M)) \wedge B$ received (A, B, L, K) B received M; 上述的两个假设表示标识 L 可关联同一轮协议的不同消息. $A9: TTP$ believes (A said $C \wedge B$ received $C \wedge TTP$ received $K) \supset TTP$ says K; 表示 TTP 只有在确信 A 已说过 C,并且 B 收到了 C,以及 TTP 收到了 K,才将 K 公布到其公开目录中. $A10: TTP$ says $X \supset P$ ftp $X \supset P$ sees X; TTP 将其认为是有效的数据放入其公共目录下,并可为任何主体通过 ftp 操作访问. $A11: P$ believes $PK_0(Q, K) \wedge P$ received $\{X\}K^{-1}$ P believes (Q said $X)$; 表示 P 如果收到一个签名消息,并且 P 相信这个签名密钥是 Q 的,那么 P 相信 Q 说过 X. 这个假设是 $P4$ 的一个扩展. $A12: A$ believes fresh (Na); $A13: TTP$ believes $\Psi \supset \Psi$.

说明协议目标

根据非否认协议所要达成的公平性和证据有效性, ZG 协议的目标描述如下:一般目标: $G1$ A believes (B received $M)$;

运用规则和公理进行推证

由消息 (1),得: $F1: B$ received $SA(f_{NRO}, B, L, C)$.

由 $F1, A2, P4, A11$ 得: $F2: B$ believes (A said $(f_{NRO}, B, L, C))$.

由 $F2, P5$,得: $F3:$ B believes $(A$ said $C)$.

同理,对原协议消息 (2) 的分析只能得到 A 相信主体 B 说过 C,而不能得到主体 A 关于 B 从 A 处接收到了 C 的信仰,故在原协议的 NRO 与 NRR 中增加新鲜随机数的挑战-质询,修改如下: $(1) A \rightarrow B: f_{NRO}, B, L, C, S_A(f_{NRO}, B, L, Na, C)$, $(2) B \rightarrow A: f_{NRR}, A, L, C, S_B(f_{NRR}, A, L, Na + 1, C)$.

对修改后的协议进行分析. 由消息 (2),得: $F4: A$ receives $S_B(f_{NRO}, A, L, Na + 1, C)$,由 $F4, A2, P4, A11, A12$,得: $F5: A$ believes (B received $(f_{NRO}, B, L, Na, C)) \supset A$ believes (B received $C)$

由消息 (3),得: $F6: TTP$ received $S_A(f_{NRS}, B, L, K)$,由 $F6, A2, A3$,得: $F7: TTP$ believes (A said $(f_{NRS}, B, L, K)) \supset TTP$ received K

根据假设 $A9$, TTP 只在确信 A 已说过 C,并且 B 收到 C,以及 TTP 收到了 K,才将 K 公布到其公开目录中,但在原有协议中, TTP 并不能确知 B 是否已收到了 C,因此, A 可对 NRR 进行签名,并将结果发给 TTP. 对消息 (3) 修改如下: $(3) A \rightarrow TTP: f_{NRS}, B, L, K, NRS\_K, S_A(NRR)$, TTP 收到消息 (3) 后由 $P5$ 得: $F8: TTP$ received $S_A(NRR)$. 由 $F8, A3, A11, P1$ 得: $F9: TTP$ believed (A said $C \wedge B$ received $C)$. 由 $F8, F9, A9, A6$,得: $F10: TTP$ says K. 由 $F10, A10$,消息 (4),得: $F11: B$ received $(f_{NRD}, A, B, L, K, S_{TTP}(f_{NRO}, A, B, L, K))$. 由 $F11, P5, A13$,得: $F12: (B$ received $K \wedge B$ received $C) \supset B$ received M. 由 $F12, P6, A7$,消息 (5) 得: $F13: A$ received $(f_{NRD}, A, B, L, K, S_{TTP}(f_{NRO}, A, B, L, K))$. 由 $F10, F12, F13, A5, A11, P5, P7, P10$,得:

$F14: A$ believes (TTP says $K) \supset A$ believes (B sees $K) \supset A$ believes (B received $M)$.

得证 $G1$.

由 $F7, F11, A5$,得: $F15: B$ believes (TTP says $K) \supset B$ be-

lieves(*A* said *K*). 由 *F*3, *F*15,得: *F*16: *B* believes(*A* said *M*).

得证 *G*2.

由 *F*14, *F*16,可得修改后的协议的一般目标是满足的,即协议任何一步执行后通信双方主体的地位是公平的.

如果出现主体否认其协议行为,并引发纠纷,双方则可按要求向仲裁 *J* 出示证据,通过证明协议仲裁目标的满足与否来检验主体的否认行为的非否认性. 我们假设 *J* 相信主体 *A*, *B*,和 *TTP* 的签名私钥,并且知道与私钥对应的主体的公钥.

协议可能出现的纠纷及解决,分以下两种情况:

case1　*A* 否认向 *B* 发送了消息 *M*. 在这种情况下 *B* 可将 *M*, *C*, *K*, *L*,以及 *NRO*, *NRD*. *K* 提交给仲裁,仲裁通过以下几步可证明 *A* 发送了消息 *M*.

(1) 检查 *NRD*. *K* 是用 *T* 的私钥对消息(f_{NRO}, *A*, *B*, *L*, *K*)的签名;

J received $S_{TTP}(f_{NRO}, A, B, L, K) \supset J$ believes (*TTP* says *K*) $\supset J$ believes (*A* said *K*)

(2) 检查 *NRO* 是用 *A* 的私钥对消息(f_{NRO}, *B*, *L*, *Na*, *C*)的签名;

J received $S_A(f_{NRO}, B, L, Na, C) \supset J$ believes (*A* said *C*)

(3) 如果检查 $M = D(K: C)$,则:

J believes (*A* said *M*)

得证 *G*3.

case2　*B* 否认收到了消息 *M*. 在这种情况下 *A* 将 *M*, *C*, *K*, *L* 以及 *NRR*, *NRD*. *K* 提交给仲裁,仲裁通过以下几步可证明 *B* 接收到了消息 *M*.

(1) 检查 *NRD*. *K* 是用 *T* 的私钥对消息(f_{NRO}, *A*, *B*, *L*, *K*)的签名;

J received $S_{TTP}(f_{NRO}, A, B, L, K) \supset J$ believes (*TTP* says *K*) $\supset J$ believes (*B* received *K*)

(2) 检查 *NRR* 是用 *B* 的私钥对消息(f_{NRO}, *A*, *L*, *Na* + 1, *C*)的签名;

J received $S_B(f_{NRO}, A, L, Na + 1, C) \supset J$ believes (*B* received *C*)

(3) 如果检查 $M = D(K: C)$,则:

J believes (*B* received *M*)

得证 *G*4.

以上的证明表明 ZG协议能够为解决可能出现的纠纷提供有效的证据.

修改后的协议为:

(1) $A \rightarrow B: f_{NRO}, B, L, C, S_A(f_{NRO}, B, L, Na, C)$

(2) $B \rightarrow A: f_{NRR}, A, L, C, S_B(f_{NRO}, A, L, Na + 1, C)$

(3) $A \rightarrow TTP: f_{NRS}, B, L, K, NRS. K, S_A(NRR)$

(4) $B \leftrightarrow TTP: f_{NRD}, A, B, L, K, NRD. K$

(5) $A \leftrightarrow TTP: f_{NRD}, A, B, L, K, NRD. K$

4　结束语

本文我们运用 SVO 逻辑对一个非否认协议实例-ZG协议的公平性与证据有效性进行了形式化分析,使非否认协议的多种性质的分析得以在同一形式化验证框架下进行,并修改了 ZG协议存在的漏洞. 非否认协议具有较大的应用价值,ZG协议为非否认协议的设计提供了一个极好的思路,因此对 ZG协议进行严格的形式化分析,验证其正确性是十分必要的. 如何建立此类协议的形式化分析工具的良好语义模型,并进行严格的理论推证需要进一步的工作.

参考文献:

[1] J Zhen, D Gollmann. A fair non-repudiation protocol. In IEEE Computer Society Symposium on Research in Security and Privacy, 1996.

[2] M Abadi, A Gordon. A calculus for Cryptographic protocols: The spi calculus. Information and Computation, 1998.

[3] Schneider S. Verifying Authentication Protocols with CSP, Proceedings of the IEEE Computer Security Foundations Workshop X, (1997) 3 - 17, IEEE Computer Society Press.

[4] P F Syverson, P C van Oorschot. A Unified Cryptographic Protocol Logics. In Proceedings of the 1994 IEEE Computer Society Press, 1994.

[5] E F Brickell, D Chaum, I B Damgard, J van de Graaf. Gradual and verifiable release of a secret. Lecture-Notes in Computer Science 293, Advances in Cryptology: Proceedings of Crypto '87, pages 156 - 166, Santa Barbara, CA Auguest, 1987.

作者简介:

范　红　女,1969 年 7 月出生于河北保定,博士研究生,研究方向为信息安全,在国内外刊物上发表论文 20 余篇,专著 3 本. E-mail: pkfanhong@sina.com

冯登国　男,1965 年 5 月出生,陕西靖边人,研究员,博士导师,中科院信息安全国家重点实验室主任,国家信息安全 863 项目专家组组长,研究方向为信息安全,在国内外刊物上发表论文近 200 篇,专著 15 本.