非否认协议中认证保密性的设计与形式化分析*)

张 虹
(潍坊学院计算机与通信工程学院 潍坊 261061)

摘 要 探讨了非否认协议的保密性认证目标,用攻击的方法验证了 A(0)协议在认证保密性方面的不足;对其消息格式和会话密钥建立后确认方式做了修改,提出了 NA(0)协议;进一步运用 SVO 逻辑对 NA(0)协议进行了形式化的分析,验证了 NA(0)协议满足主体身份的认证性和会话密钥的保密性。

关键词 非否认协议,认证保密性,形式化分析,SVO 逻辑

Design and Formal Analysis of Secrecy in the Non-repudiation Protocol

ZHANG Hong
(School of Computer and Communication Engeering, Weifang University, Weifang 261061, China)

Abstract On the basis of discussing the secrecy goals of non-repudiation protocol, the papar validateed the shortages of A(0) protocol by the means of aggressing, revamped the affirmance fashion of its information format and conversation encrypting keys, and lodged NA(0) protocol. Then the NA(0) protocol was analysed formally by SVO logic, and it was validated fulfilling the authentication of main identity and secrecy of conversation.

Keywords Non-repudiation protocol, Secrecy, Formal analysis, SVO Logic

1 序言

非否认技术作为网络安全中最具价值的研究问题之一,在避免电子商务参与主体因事后否认所进行的交易行为而给对方造成损失方面起着重要的作用。非否认协议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交易行为,即达成协议的非否认性[1]。非否认协议的目标有两个:一个是确认发方非否认,亦即非否认协议向接收方提供不可抵赖的证据,证明收到消息的来源的可靠性;另一个是确认收方非否认,亦即非否认协议向发送方提供不可抵赖的证据,证明接收方已收到了某条消息。电子商务协议的目标除认证性、非否认性之外,还有可追究性、公平性等。而一个良好且安全的非否认协议是完成电子商务交易的必要条件[2]。本文主要对非否认协议中的认证保密性进行了探讨,分析主体身份的认证性和临时会话密钥的保密性内涵,指出了 A(0)协议存在的漏洞,对其消息格式和会话密钥建立后确认方式做了修改,并应用 SVO 逻辑对修改后的协议进行了形式化的分析[3],验证了它满足主体身份的认证性和临时会话密钥的保密性。

2 认证保密性

在计算机网络和分布系统中,当进行资源访问或通信时,一方主体往往需要证实另一方主体的身份。有时还要在主体之间分配密钥或其他各种秘密,认证协议就是用来描述主体之间如何证实身份以及分配秘密的,通常由一系列主体之间交换的信息组成。认证可能牵涉两方或多方主体;可能是单向认证或相互认证;可能使用对称密钥系统或非对称密钥系统。非否认协议与认证协议一样,需要在主体之间认证身份和分配密钥,它们对认证保密性的要求是一致的。因此,可以通过对认证协议进行设计和形式化分析,来讨论非否认协议的认证保密性。

3 认证保密性的设计

认证协议是网络安全性的基础,即使建立在完美密码系统上的认证协议,仍然可能存在各种各样的安全漏洞。认证协议设计与分析的困难性在于:(1)安全目标本身的微妙性;(2)协议运行环境的复杂性;(3)攻击者模型的复杂性;(4)认证协议本身的高并发性。本文以下部分将通过 A(0)协议及其改进协议的设计和形式化分析来讨论认证保密性。

3.1 A(0)协议

A(0)协议是 Matsumoto, Takashima 和 Imai 通过修改 Diffie-Hellman 密钥交换协议得到的一种密钥协商协议。A(0)协议的目的是为通信双方建立共享密钥,其特点是公平、简洁,用户不需要进行任何签名计算。主体之间的会话密钥是通过协议双方共同协商产生的,它具有减轻认证中心负担和限制认证中心权限的优点。作为协议的前提,首先得选定公开的大素数 P 和有限域 $GF(P)$ 上的本原元 a。在协议开始之前,通信双方 A 和 B 各自选取随机整数 $\bar{x}$ 和 $\bar{y}$,将计算所得的 $\overline{R_a}=a^{\bar{x}} \pmod P$(对 A 而言),$\overline{R_b}=a^{\bar{y}} \pmod P$(对 B 而言)发往认证中心 T,以获得各自的公开协商密钥证书。该证书是认证中心 T 对任一主体 C 的身份及其公开协商密钥 $\overline{R_c}$ 进行签名的结果。然后,A 和 B 各自选择一随机整数 x 和 y,A 计算 $R_a=a^x \pmod P$,B 计算 $R_b=a^y \pmod P$,所得的 R_a 和 R_b 分别称为 A 和 B 的临时公开协商密钥。在此基础上,即可执行 A(0)协议。具体的 A(0)协议如下:

① $A \rightarrow B: A, \overline{R_a}, \{A, \overline{R_a}\}_{K_i^{-1}}, R_a$

② $B \rightarrow A: B, \overline{R_b}, \{B, \overline{R_b}\}_{K_i^{-1}}, R_b$

*)山东省科技攻关项目(2007GG30003003)。张 虹 副教授,主要研究方向为信号检测、参数估计、数字通信、并行信号处理。

其中，$\{A,\overline{R_a}\}_{K_t^{-1}}$ 是认证中心 T 签发的、主体 A 的公开协商密钥证书。B 收到消息①后，通过验证 T 的签名证实 A 的身份，进而计算出 $K_{ab}=(\overline{R_a})^y\cdot(R_a)^{\bar{y}}=a^{\overline{xy}}\cdot a^{\bar{xy}}$ 作为与 A 之间的共享会话密钥。A 也可以类似地验证 B 的身份，并获得他与 B 之间的共享会话密钥：$K_{ab}=(\overline{R_b})^x\cdot(R_b)^{\bar{x}}=a^{\overline{xy}}\cdot a^{\bar{xy}}$。最终，$A$，$B$ 通过执行 A(0)协议建立了他们之间的会话密钥 K_{ab}。

3.2 A(0)协议的改进协议 NA(0)[3]

迄今为止已发现多种对 A(0)协议的攻击方法。最常见的攻击方法为[4]：攻击者 P 先于 A 进行正常通信，发起协议的第一轮执行：

(1) $P\rightarrow A:P,\overline{R_P},\{P,\overline{R_P}\}_{K_t^{-1}},R_P$

(2) $A\rightarrow P:A,\overline{R_a},\{A,\overline{R_a}\}_{K_t^{-1}},R_a$

然后，P 将 A 发送给他的消息转发给 B，发起协议的第二轮执行，并将 B 发送给 A 的消息截获。

① $P(A)\rightarrow B:A,\overline{R_a},\{A,\overline{R_a}\}_{K_t^{-1}},R_a$

② $B\rightarrow P(A):B,\overline{R_b},\{B,\overline{R_b}\}_{K_t^{-1}},R_b$

其中，P：攻击者，$P(A)$：攻击者 P 伪冒 A。这样，B 就会错误地认为它与 A 之间已经共享一个会话密钥：$K_{ab}=(\overline{R_a})^y\cdot(R_a)^{\bar{y}}$。而 A 对此却一无所知，因为他此时只与 P 共享会话密钥 $K_{aP}=(\overline{R_P})^x\cdot(R_P)^{\bar{y}}$。由此可知，A(0)协议失败，攻击者 P 获得成功。

从以上攻击方法可知，攻击者主要利用 A(0)协议消息格式的同一性、协议主体不能区分协议的发起方和响应方而进行了有效的攻击。要确保协议的安全，首先得修改协议的消息格式，使得协议能够区分发起方和响应方，并且在会话密钥建立后进行握手确认，使得协议双方都确定对方已拥有协商的会话密钥。针对 A(0)协议的缺点，对其进行改进得到的 NA(0)协议如下：

(1) $A\rightarrow B:N_a,A,\overline{R_a},\{A,\overline{R_a}\}_{K_t^{-1}},R_a$

(2) $B\rightarrow A:B,\overline{R_b},\{B,\overline{R_b}\}_{K_t^{-1}},R_b,\{N_a,B,N_b\}_{K_{ab}}$

(3) $A\rightarrow B:\{N_a,A,N_b\}_{K_{ab}}$

其中，$N_a=H(Date\ Time\ A)$，为 A 生成的 P 随机数的惟一标识本次协议的运行[5]，N_a 把协议中交互信息联系在一起。*Date Time A* 标志着主体 A 本次协议发起的时间。$N_b=H(Date\ Time\ B)$，为 B 生成的随机数用以标识本次协议协商的密钥的新鲜性，*Date Time B* 标志着主体 B 接受本次协议的时间。H 为强单向无碰撞函数。不同的 *Date Time* 有不同的 $H(Date\ Time)$随机数。协议中使用 *Date Time* 是为了具有抵抗拒绝服务攻击的能力。攻击者如果想让协议主体浪费很多的时间在无用的等待上而无法为诚实的主体提供服务，主体可以根据自己的 *Date Time* 取消长时间等待的协议的执行，使得攻击失败。

3.3 NA(0)协议的分析

NA(0)协议的执行前提非常简单：只需有一个证书颁发中心。协议参与方获得各自的证书后就可以与自己想通信的人执行 NA(0)协议来获得一个双方共享的临时密钥，然后就可以使用这个临时的密钥进行通信。NA(0)协议对消息的格式做了很好的调整，使得每一步消息都能自包含协议的步骤信息，而且能避免类型缺陷攻击。NA(0)协议简洁、高效，密钥的建立一共只需执行 3 步，并且没有冗余信息。NA(0)协议通过把协议发起通信时间和接受通信时间信息包含在协议信息中，使得协议具有抵抗拒绝服务攻击的能力。此外，通过对 NA(0)协议进行形式化的分析，还可知它具有抵抗重放和伪冒攻击的能力。

4 认证保密性的形式化分析

认证保密性的设计和分析是一项十分困难的任务。即使只讨论最基本的认证协议，协议的参与主体只有两三个，交换的消息只有 3 至 5 条，要设计一个正确的、符合认证目标的、没有冗余的认证协议也十分困难。因此迫切需要一种合适的形式化分析工具，对协议中的认证保密性进行严谨的形式化分析，检查认证保密性是否达到，协议中是否存在安全缺陷和冗余。

分析安全协议最直接、最简单的方法是基于知识与信念推理的模态逻辑方法。它们由一些命题和推理规则组成。命题表示主体对消息的知识或信念，而应用推理规则可以从已知的知识和信念推导出新的知识和信念。在这类方法中，最著名的是 BAN 类逻辑，其中包括 BAN 逻辑、GNY 逻辑、AT 逻辑、VO 逻辑和 SVO 逻辑。SVO 逻辑吸取了 BAN 逻辑、GNY 逻辑、AT 逻辑、VO 逻辑的优点，将它们集成在一个逻辑系统中。在形式化语义方面，SVO 逻辑对一些概念做了有别于 AT 逻辑的重新定义，从而取消了 AT 逻辑系统中的一些限制。

4.1 SVO 逻辑

SVO 逻辑所用的记号与 BAN 类逻辑相似，其中特有的符号共有 12 个。应用 SVO 逻辑对安全协议进行形式化分析可以分为 3 个步骤[7]：

(1)给出协议的初始化假设集合 Ω，即用 SVO 逻辑语言表示出各主体的初始信念、接收到的消息、对所收到消息的理解和解释；

(2)给出协议可能或应该达到的目标集 Γ，即用 SVO 逻辑语言表示一个公式集；

(3)在 SVO 逻辑中证明结论 $\Omega\vdash\Gamma$ 是否成立。若成立，则说明该协议达到了预期的设计目标，协议的设计是成功的。

SVO 逻辑是 BAN 类逻辑中的佼佼者，它的理论基础更加坚实，在实用上仍然保持了 BAN 逻辑简单、易用的特点，因此被广泛接受。应用 SVO 逻辑，不仅成功分析了各种认证协议，也成功地分析了在电子商务中应用日益广泛的非否认协议的保密性。

SVO 逻辑遵从两条推理规则和 10 个公理。两条推理规则为：

MP 规则：由 φ 和 $\varphi\supset\psi$ 可以推导出 ψ；

Nec 规则：由 $\vdash\varphi$ 可以推导出 $\vdash P\models\varphi$。

其中，φ 和 ψ 是公式，P 表示主体，$\vdash\varphi$ 表示 φ 是一个可由公理推导而来的公式。

10 个公理[6]是：信任公理、消息来源公里、密钥协商公理、接受公理、消息拥有公理、消息理解公理、管辖公理、消息新鲜性公理、临时值验证公理、“好的”共享密钥对称性公理。此处列出的只是与证明有关的公理。

4.2 NA(0)协议的形式化分析

为验证修改后协议的安全性，现使用 SVO 逻辑进行形式化的分析。对协议的发起方 A 和接收方 B 进行分析如下：

(Ⅰ)对于主体 A

关于主体 A 的初始假设集合：

$P_1:A\models PK_a(T,K_t)$，

$P_2:A\models A\ni(\overline{R_a},R_a,\bar{x},x)$，

$P_3: A \models SV(\{B,\overline{R_b}\}_{K_i^{-1}}, K_i, (B,\overline{R_b}))$,

$P_4: A \models EV((N_a,B,N_b), K_{ab}, \{N_a,B,N_b\}_{K_{ab}})$,

$P_5: A \models PK_\delta(A,(\overline{R_a},R_a))$,

$P_6: A \models \#(R_a)$,

$P_7: A \models ((T \mid\sim PK_\delta(B,\overline{R_b}) \wedge A \lhd ((B,\overline{R_b},\{B,\overline{R_b}\}_{K_i^{-1}}), *_b) \wedge EV((N_a,B,N_b), K_{ab}, \{N_a,B,N_b\}_{K_{ab}})) \supset PK_\delta(B,(\overline{R_b},*_b)))$,

$P_8: A \lhd (B,\overline{R_b},\{B,\overline{R_b}\}_{K_i^{-1}}, R_b, \{N_a,B,N_b\}_{K_{ab}})$,

$P_9: A \models A \lhd (B,\overline{R_b},\{B,\overline{R_b}\}_{K_i^{-1}}, R_b, \{N_a,B,N_b\}_{K_{ab}})$,

$P_{10}: A \models (T \mid\sim (B,\overline{R_b}) \supset T \mid\sim PK_\delta(B,\overline{R_b}))$,

$P_{11}: A \models (B \mid\sim (N_a,B,N_b) \supset B \models B \overset{K_{ab}-}{\longleftrightarrow} A \wedge B \mid\sim (B \ni K_{ab}) \wedge B \models \#(K_{ab}))$。

P_1 至 P_7 反映了主体 A 的初始信念，P_8 接收消息，P_9 理解消息，P_{10}，P_{11} 解释消息。另外，对 SVO 逻辑做了点补充，引入 $EV(X,K,Y)$ 表示用加密密钥 K 对 X 加密的结果是 Y。

协议目标：

$G_1: A \equiv \overset{K_{ab}+}{\longleftrightarrow} B$

$G_2: A \mid\equiv \#(K_{ab})$

运用规则和公理进行推证。

首先写出各个步骤所得到的结果，然后给出推导该结果时所用到的规则、公理、公式和初始假设。

(1)$A \models (A \lhd \{B,\overline{R_b}\}_{K_i^{-1}})$，由 P_8、接受公理和 Nec 规则可得。

(2)$A \models (T \mid\sim (B,\overline{R_b}))$，由式(1)、$P_1$、$P_3$ 和消息来源公理可得。

(3)$A \models T \mid\sim PK_\delta(B,\overline{R_b})$，由式(2)、信任公理和 MP 规则可得。

(4)$A \models PK_\delta(B,(\overline{R_b},*_b))$，由式(3)、$P_9$、$P_4$、信任公理、$P_7$ 和 MP 规则可得。

(5)$A \models A \overset{K_{ab}}{\longleftrightarrow} B$，由式(4)、$P_5$、密钥协商公理、信任公理和 MP 规则可得。其中 K_{ab} 如式(6)所示。

(6)$K_{ab} = F_0(\overline{R_a},R_a,\overline{R_b},*_b) = (\overline{R_b})^x \cdot (R_b)^{\bar{x}} = (\overline{R_a})^y \cdot (R_a)^{\bar{y}} = g^{\tilde{xy}+\tilde{x}\tilde{y}} \pmod P$。

(7)$A \models \#(K_{ab})$，由式(6)、P_6、消息新鲜性公理可得。目标 G_2 达到。

(8)$A \models A \ni (\overline{R_b},*_b)$，由 P_9、消息拥有公理、信任公理 MP 规则可得。

(9)$A \models A \in K_{ab}$，由式(8)、P_2、式(6)和消息拥有公理可得。

(10)$A \models A \overset{K_{AB}-}{\longleftrightarrow} B$，由式(5)、式(9)和 $A \overset{K_{AB}-}{\longleftrightarrow} B$ 的定义，应用信任公理和 MP 规则可得。

(11)$A \models (A \lhd \{N_a,B,N_b\}_{K_{ab}})$，由 P_8、接受公理和 Nec 规则可得。

(12)$A \models B \mid\sim (N_a,B,N_b)$，由式(5)、式(1)和消息来源公理可得。

(13)$A \models B \mid\sim (B \ni K_{ab})$，由式(12)、$P_{11}$、信任公理和 MP 规则可得。

(14)$A \models B \mid\approx (B \ni K_{ab})$，由式(7)、消息新鲜性公理、式(13)、临时值验证公理、信任公理和 MP 规则可得。

(15)$A \models A \overset{K_{ab}+}{\longleftrightarrow} B$，由式(10)、式(13)和 $A \overset{K_{ab}+}{\longleftrightarrow} B$ 的定义可得。目标 G_1 达到。

由式(7)和式(15)可知，协议目标 G_1 和 G_2 都已达到。

(Ⅱ)对于主体 B

主体 B 收到的第一条消息和第二条消息合并就对应于主体 A 收到的消息。由对称性可得，协议可达到以下目标：

$G_3: B \equiv B \overset{K_{ab}+}{\longleftrightarrow} A$

$G_4: B \models \#(K_{ab})$

由(Ⅰ)和(Ⅱ)可知，修改后的协议满足安全性目标。

这一结论表明：成功执行完修改后的 A(0)协议，主体 A 和主体 B 都相信 K_{ab} 是他们共同拥有的、其他人不知道的而且是双方都相信是新鲜性的会话密钥。因此说，改进后的 A(0)协议完成了明确的密钥认证，从而达到了理想的认证目标。

结束语 对 A(0)协议进行了分析，并用攻击的方法验证其在认证保密性方面的不足。然后对 A(0)协议进行了改进，提出了 NA(0)协议。进一步运用 SVO 逻辑对 NA(0)协议进行形式化的分析，验证了 NA(0)协议达到了协议主体身份认证和临时会话密钥的保密性的目的。通过分析和修改 A(0)协议，阐述了非否认协议的认证保密性。

需要指出的是，现有的形式化分析方法还很不完善，它们都只能发现协议的缺点，而不能保证经过分析没有问题的协议一定是安全的、不存在攻击的。所以，现有的形式化分析方法还有待于进一步的深入和完善。

参 考 文 献

[1] Zhou J, Gollmann D. A Fair Non-repudiation Protocol// Symposium on Security and Privacy. Oakland, CA, USA, IEEE Computer Society, 1996: 55-61

[2] Schneider S. Formal Analysis of a Non-repudiation Protocol// IEEE Computer Secutity Foundations Workshop. Los Alamitos, CA, USA, IEEE. Computer Society, 1998: 54-65

[3] 蔡永泉，朱勇. 一种改进的 A(0)协议及其形式化分析. 计算机工程与应用，2006，42：109-111

[4] Ezhilchelvan P D, Shrivastava S K. A Family of Trusted Third Party Based Fair-exchange Protocols. IEEE Transactions on Dependable and Secure Computing, 2005, 2: 273-286

[5] 卿斯汉，李改成. 公平交换协议的一个形式化模型. 中国科学 E 辑 信息科学，2005，35(2)：161-172

[6] 卿斯汉. 安全协议. 清华大学出版社，2005，3：101-185

[7] 卿斯汉. 安全协议 20 年研究进展[J]. 软件学报，2003，14 (10)：1740-1752