安全协议的设计与逻辑分析*

卿斯汉+

(中国科学院 信息安全技术工程研究中心,北京 100080)
(中国科学院 软件研究所 信息安全国家重点实验室,北京 100080)

Design and Logical Analysis of Security Protocols

QING Si-Han+

(Engineering Research Center for Information Security Technology, The Chinese Academy of Sciences, Beijing 100080, China)
(State Key Laboratory of Information Security, Institute of Software, The Chinese Academy of Sciences, Beijing 100080, China)
+ Corresponding author: Phn: 86-10-62635150, Fax: 86-10-62635150, E-mail: qsihan@yahoo.com
http://www.ercist.iscas.ac.cn
Received 2003-01-23; Accepted 2003-04-07

Qing SH. Design and logical analysis of security protocols. *Journal of Software*, 2003,14(7):1300~1309.
http://www.jos.org.cn/1000-9825/14/1300.htm

Abstract: With the rapid growth of network applications, network security has become an important issue. In this paper, the following issues are investigated: the design principles of security protocols, the use of formal methods in the design of security protocols, the characteristics of various approaches to formal analysis, in particular logical analysis. The strand space approach to logical analysis, and the possibility of the strand space model guiding the formal design of security protocols are also explored.
Key words: security protocol; design; logical analysis; BAN-like logic; strand space

摘 要: 随着网络应用的迅速发展,网络安全的问题日益重要.研究下述课题:安全协议的设计原则;安全协议设计中形式化方法的应用;各种形式化分析方法,特别是逻辑分析方法的特点.另外,还探讨了串空间模型在逻辑分析中的应用以及串空间模型指导安全协议形式化设计的可能性.
关键词: 安全协议;设计;逻辑分析;BAN 类逻辑;串空间
中图法分类号: TP309 **文献标识码**: A

密码学是网络安全的基础,但网络安全不能单纯依靠安全的密码算法.安全协议是网络安全的一个重要组成部分,我们需要通过安全协议进行实体之间的认证、在实体之间安全地分配密钥或其他各种秘密、确认发送和接收的消息的非否认性等.近年来,安全协议越来越多地用于保护因特网上传送的各种交易,保护针对计算机系统的访问.但是,经验告诉我们,设计和分析一个正确的安全协议是一项十分困难的任务.即使我们只讨论安全协议中最基本的认证协议,其中参加协议的主体只有两三个,交换的消息只有 3~5 条,设计一个正确的、符合

* Supported by the National Natural Science Foundation of China under Grant No.60083007 (国家自然科学基金); the National Grand Fundamental Research 973 Program of China under Grant No.G1999035810 (国家重点基础研究发展规划(973))

第一作者简介: 卿斯汉(1939－),男,湖南隆回人,研究员,博士生导师,主要研究领域为信息系统安全理论和技术.

认证目标的、没有冗余的认证协议也很不容易[1,2].因此,我们必须借助形式化的分析工具,证明安全协议的正确性.自 20 世纪 70 年代以来,安全协议的形式化分析已逐渐成为信息安全研究领域中的一个热点,涌现出众多的研究方法.目前,研究比较广泛和深入的方法主要有以下 4 种:基于知识与信念推理的模态逻辑方法、基于通信状态机模型的研究方法、基于知识推理的代数方法和基于顺序通信进程的 CSP 方法[3].近年来,串空间模型[4,5]方法的应用日益广泛.

本文第 1 节讨论基于知识与信念推理的模态逻辑方法,对 BAN 逻辑[6]及其重要的增强与扩展——GNY 逻辑[7]、AT 逻辑[8]、VO 逻辑[9]——进行详尽的研究,比较它们的特点和优缺点.第 2 节讨论 BAN 类逻辑中的佼佼者——SVO 逻辑[10],并研究安全协议的逻辑分析方法和串空间模型[4,5]相结合的问题.第 3 节讨论安全协议的设计原则.设计时必须充分考虑 Dolev-Yao[11]攻击者模型,不低估攻击者的能力.安全协议必须能够抵抗常见攻击,特别是重放攻击[12,13].然后,通过串空间模型的实例,说明形式化方法如何指导安全协议的正确设计.第 4 节是简短的结论,并讨论今后研究的若干方向.

1 安全协议的形式化分析方法

1.1 基于知识与信念推理的模态逻辑方法

模态逻辑方法是分析安全协议的最为重要的方法之一,它们分析并验证了许多重要的安全协议[14],其中包括分析经典的 Needham-Schroeder 私钥协议[15]、Lowe-Needham-Schroeder 公钥协议[16]、Nessett 协议[17]等.

模态逻辑分析方法与分布式系统中分析知识和信念演化的逻辑相似.这些逻辑系统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,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.Syverson 在文献[18]中阐述了在安全协议的分析中,知识、信念和语义之间关系的相互作用.

在这类方法中,最著名的是 BAN 类逻辑[6~10].其他相近的工作还包括:Bieber 逻辑——CKT5[19]、Syverson 逻辑——KPL[20]、Rangan 逻辑[21]、Moser 逻辑[22]以及 Yahalom,Klein,Beth 的 YHK 逻辑[23]等.1999 年,Kindred 在他的博士论文[24]中提出的密码协议的生成理论——RV 逻辑是这方面的又一个新成果.

Syverson 逻辑将攻击者具有的知识分为两类:一类是攻击者收到一条消息后所具有的知识(在看见一个比特串的含义下);另一类是攻击者可以识别消息时所具有的知识.然后,Syverson 逻辑可以对此进行推理.类似于 Syverson 逻辑,Bieber 逻辑也区别看见一条消息和理解一条消息,并能对安全协议中知识的演化进行推理.Rangan 逻辑的特点是研究可信(trust),对由“可信”到“信念”(belief)的演化过程进行推理.YKB 逻辑则从另一个角度讨论“可信”.在上述逻辑中,知识和信念的演化都是单调的,亦即知识和信念的演化只增不减.Moser 逻辑是惟一的例外,它的信念演化是非单调的.例如,在推理过程中如果知道一个密钥已被泄露,则其信念集合可以减小.

BAN 逻辑之所以著名,不仅由于它开创了安全协议形式化分析的先河,是一项开拓性的工作,而且由于它提供的形式化分析方法特别直观与简单.有人说,BAN 逻辑成功的秘诀是“简单加实用”,这话有一定的道理.BAN 逻辑虽然简单,但仍然可以成功地揭示安全协议中的设计缺陷.例如,通过 BAN 逻辑分析,发现了 CCITT X.509 标准[25]推荐草案中的安全漏洞.

BAN 逻辑的直观性与简单性主要表现在以下几个方面:第 1,BAN 逻辑不区分看见一条消息和理解一条消息;第 2,BAN 逻辑的信念演化过程是单调递增的;第 3,BAN 逻辑不讨论“可信”;第 4,BAN 逻辑不讨论知识;第 5,BAN 逻辑假设参加协议的主体是诚实的,他们都忠实地根据协议的规则执行协议;第 6,BAN 逻辑假设加密系统是完善的(perfect)等等.

但是,BAN 逻辑不追求完美而追求简洁、实用的设计思想,也为 BAN 逻辑分析方法带来了局限性,使 BAN 方法的抽象级别过高,分析范围过窄.例如,由于 BAN 逻辑不能对知识进行推理,因此,BAN 逻辑只能分析协议的认证性质,而不能分析协议的保密性质.然而在现实中,通常的密钥分配协议要同时实现保密性和认证性两个重要目标.

1.2 BAN逻辑

BAN 逻辑是一种多类型模态逻辑(many-sorted modal logic),它包含以下 3 种处理对象:主体、密钥和公式.其中的公式,也称作语句或命题.BAN 逻辑仅包含合取这一命题联接词,用逗号表示.BAN 逻辑共有 19 条推理规则.在推理规则中,$\vdash$是元语言符号. $\Gamma \vdash C$ 表示可以由前提集 Γ 推导出结论 C.应用 BAN 逻辑形式化分析安全协议的步骤是:

1. 对安全协议进行理想化,亦即,将协议消息转换为 BAN 逻辑所能理解的公式;
2. 对安全协议进行解释,亦即,将形如 $P \to Q: X$ 的消息转换成形如 Q received X 的逻辑语言.解释过程中遵循以下规则:

(1) 若命题 X 在消息 $P \to Q: Y$ 前成立,则在其后,X 和 Q received Y 都成立;

(2) 若根据推理规则可以由命题 X 推导出命题 Y,则命题 X 成立时,命题 Y 亦成立;

3. 应用 BAN 逻辑语言对系统的初始状态进行描述,给出初始化假设集;
4. 应用 BAN 推理规则对协议进行形式化分析,得出相应的结论.

关于 BAN 逻辑的其他内容,例如 BAN 逻辑构件的语法和语义、BAN 逻辑的推理规则、BAN 逻辑分析认证协议的实例等,读者可参见其他文献,例如文献[1,2].

1990 年,Nessett[17]引入一个简单的例子,试图说明 BAN 逻辑本身存在一个重要的安全问题.

Nessett 协议如下:

1. $A \to B: \{N_a, K_{AB}\}_{K_A^{-1}}$,
2. $B \to A: \{N_b\}_{K_{AB}}$.

在消息 1 中,A 用其秘密密钥加密 A 与 B 之间的会话密钥和临时值 N_a,然后发送给 B.B 用 A 的公开密钥 K_A 解密出 K_{AB},然后用 K_{AB} 加密临时值 N_b 后发送给 A,显然, K_{AB} 不是 A 和 B 之间通信的“良好”的会话密钥,因为任何主体都可以从消息 1 中获得会话密钥 K_{AB}.但是,用 BAN 逻辑分析 Nessett 协议,却得出 K_{AB} 是良好的会话密钥的结论.

据此,Nessett 认为,BAN 逻辑本身存在一个重要缺陷,该缺陷源于 BAN 逻辑的分析范围.因为 BAN 逻辑只考虑分配密钥和身份认证的问题,但未考虑哪个主体不应当获得密钥,亦即,未考虑机密性的问题.

BAN[26]对 Nessett 的批评答复如下:在 BAN 逻辑的文献中,已经清楚地说明,BAN 逻辑只讨论诚实主体的认证问题,并不关心检测非授权地暴露秘密的问题.在 Nessett 协议中,A 在消息 1 中公开了 K_{AB},故 Nessett 的假定: A believes $A \xleftrightarrow{K_{AB}} B$ 不符合 BAN 的基本假定.因此,Nessett 从不合理的初始假定推导出了不合理的结论,而 BAN 逻辑本身并不能防止建立不合理的初始假定集合.

虽然我们不能通过 Nessett 协议说明 BAN 逻辑本身存在着缺陷,但 Nessett 的反例启示我们,BAN 逻辑的推理分析依赖于我们所作的基本假设和初始假设.如果非形式化的初始假设错了,则通过形式化分析之后常常得出错误的结论.

1.3 GNY逻辑、AT逻辑和VO逻辑

在对 BAN 逻辑进行增强和扩充的过程中,GNY 逻辑、AT 逻辑、VO 逻辑和 SVO 逻辑最为著名,习惯上统称它们为 BAN 类逻辑.其中,SVO 逻辑是在总结 BAN 逻辑、GNY 逻辑、AT 逻辑和 VO 逻辑的基础上发展起来的,我们将在下一节加以讨论.

(1) GNY 逻辑

BAN 逻辑问世以后,第一个对它进行增强的是 GNY 逻辑.GNY 的逻辑公设有 44 个之多.此外,在 GNY 逻辑中,如果 $\frac{C_1}{C_2}$ 是逻辑公设,则对任何主体 P, $\frac{P \models C_1}{P \models C_2}$ 也是逻辑公设.

具体地说,在 GNY 逻辑中,有接收法则 6 个(T1~T6);拥有法则 8 个(P1~P8);新鲜性法则 11 个(F1~F11);识别法则 6 个(R1~R6);消息解释法则 7 个(I1~I7);管辖法则 3 个(J1~J3);“不在这里产生”法则 3 个.

GNY 逻辑对 BAN 逻辑的重要改进与推广有以下几个方面:(1) 通过新增加的逻辑构件与法则,推广了

BAN 逻辑的应用范围.例如,GNY 逻辑不局限于分析认证协议,还可以分析某些应用单向函数的密码协议;(2) 增加了“拥有密钥”的表达式,增强了 GNY 逻辑本身的表达能力.因此,A 相信 C 拥有 A 和 B 之间的共享密钥可以表示为 A believes C has K_{AB},并能进行相应的推理;(3) 在 GNY 逻辑中,区分一个主体收到的消息和一个主体可用的消息;(4) 在 GNY 逻辑中,进一步区分一个主体自己生成的消息和其他消息;(5) 在 GNY 逻辑分析中,在理想化协议中保留明文.而在 BAN 逻辑分析中,明文在认证过程中不起作用.

类似于 BAN 逻辑,为了简化分析过程,在 GNY 逻辑中不包含否定形式,也没有粒度更细的时序概念.此外,GNY 逻辑的语义也与 BAN 逻辑相似.

尽管 GNY 逻辑具有上述特点,但它本身过于复杂.在它的 44 个法则中,有许多法则使 GNY 逻辑本身不必要地复杂.因此许多学者认为,应用 GNY 逻辑分析安全协议在实际上是行不通的.

尽管如此,我们认为,GNY 逻辑在历史的长河中发挥了它应有的作用,使我们对认证协议及 BAN 逻辑分析有了更加深刻的认识.

在 BAN 逻辑之后不久出现的 AT 逻辑为 BAN 逻辑构造了一个简单的语义模型,是对 BAN 逻辑的一种重要改进.类似于 GNY 逻辑,AT 逻辑对 BAN 逻辑的本质与局限性进行了深入的分析,并获得了相近的结论.但是,GNY 得到的是一个更加复杂的逻辑,其原因是 GNY 逻辑和 BAN 逻辑一样,缺乏一个适当的语义基础.AT 逻辑比 BAN 逻辑更接近传统的模态逻辑:它包含一个详细的计算模型,增加了模型论语义,表达能力更强,因而将 BAN 逻辑向前推进了一大步.

AT 逻辑对 BAN 逻辑的改进还包括:(1) 对 BAN 逻辑中的定义和推理法则进行整理,抛弃其中语义和实现细节的混和部分;(2) 对某些逻辑构件引入更直接的定义,免除对诚实性进行隐含假设;(3) 简化了推理法则,所有的概念都独立定义,不与其他概念相混淆;(4) 整个逻辑只有两条基本推理规则,亦即:(a) MP 规则(modus ponens):由φ和$\varphi\supset\psi$可以推导出ψ;(b) Nec 规则(necessitation):由$\vdash\varphi$可以推导出$\vdash P$ believes φ.

例如,BAN 逻辑有 P said X 的逻辑构件,说明 P 发送过 X,但没有 P 最近发送 X 的构件.在 AT 逻辑中引入了新的逻辑构件 P says X,表示 P 最近发送 X,因此更加接近新鲜性的本质.AT 逻辑的公理 A20: $fresh(X)\wedge P \text{ said } X \rightarrow P \text{ says } X$,说明若 X 是新鲜的且 P 发送过 X,则 P 最近发送了 X.这条公理更加深刻地描述了新鲜性的本质.

在 AT 逻辑中有一条比 BAN 逻辑更加直接的管辖公理 A15: $P \text{ controls } \varphi \wedge P \text{ says } \varphi \rightarrow \varphi$,说明若 P 管辖 φ 且 P 最近说过 φ,则 φ 是真实的.这个更自然的管辖内涵,使 AT 逻辑不必进行隐含的诚实性假设.

VO 逻辑的贡献是扩展了 BAN 逻辑的应用范围.Diffie-Hellman 协议[27]是许多近代密钥分配协议的基础,VO 逻辑的设计目标就是增加分析 Diffie-Hellman 协议的能力,进而可以分析 IETF 标准——因特网密钥交换协议 IKE[28]和 SSL 等.

VO 逻辑的另一个重要特点是,细化了认证协议的认证目标,给出了以下 6 种不同形式的认证目标:

(G1) Ping 认证:

$$A \text{ believes } B \text{ says } Y.$$

G1 说明 A 相信 B 最近发送过消息 Y,隐含 B 当前是激活的,亦即协议本回合开始后,B 采取了行动.注意,B 实际上想把消息 Y 发送给哪个主体是不清楚的.这类认证用于,某个主体 A 想知道他的对话方 B 是否当前是激活的.

(G2) 实体认证:

$$A \text{ believes } B \text{ says } \left(Y, R\left(G\left(R_A\right), Y\right)\right).$$

这里,R_A 表示由主体 A 生成的临时值,$G(R_A)$是 A 向 B 发出的请求.G2 说明,A 相信 B 最近发送了消息 Y,且它是对 A 的请求的响应.与 Ping 认证不同,实体认证不仅要求 A 的对话方发送一条消息,而且该消息必须与当前协议回合的会话有关,例如是对 A 的当前请求的响应.因此,A 不仅认证了 B 在 A 所执行的当前协议回合中是激活的,而且 B 参与了与 A 在当前协议回合中的对话.

(G3) 安全密钥建立:

$$A \text{ believes } A \xleftrightarrow{K-} B.$$

在 VO 逻辑中,对 BAN 逻辑中的逻辑构件 $A \xleftrightarrow{K} B$ 进行了细化.VO 认识到,AT 逻辑中的构件 A has K 表示 A 相信 K 是良好的密钥,或 K 是共享密钥等等.因此,VO 逻辑将构件 $A \xleftrightarrow{K} B$ 细化为:

• $A \xleftrightarrow{K-} B$,表示 K 是 A 的适用于 B 的未经确认的密钥.除了 A 和 B 以外,任何其他主体都不知道,也不能推导出 K.注意,这个逻辑构件强调的是,A 知道 K,但 B 未必知道 K.以 A 的观点,K 可能是一个适合 A 与 B 之间通信的良好密钥.

• $A \xleftrightarrow{K+} B$,表示 K 是 A 的适用于 B 的已经确认的密钥.A 知道 K,且 A 已经从 B 那里收到了证据(密钥确认),说明 B 确实也知道 K.其他任何主体都不知道,也不能推导出 K.

因此,在增加了这两个新的逻辑构件之后,A 和 B 的地位是不能互换的.

G3 说明,A 相信除了 B 以外,任何其他主体都不会与 A 共享密钥 K.当 B 最终获得 K 之后,A 相信 K 是 A 和 B 之间良好的会话密钥.注意,G3 并不表明 B 参加了协议的运行,也不表明 K 拥有 K.

(G4) 密钥确认:

$$A \text{ believes } A \xleftrightarrow{K+} B.$$

G4 说明,A 相信 K 是 A 和 B 之间的共享密钥,且 B 向 A 提供了知道 K 的证据.G4 表示 K 是 A 和 B 之间良好的会话密钥,且确认 B 知道 K.此时,即在 A 执行当前协议回合时,B 不但是激活的,而且 B 的身份也是确认的.

(G5) 密钥新鲜性:

$$A \text{ believes } fresh(k).$$

G5 说明,A 相信密钥 K 是新鲜的.

(G6) 互相信任共享密钥:

$$A \text{ believes } B \text{ believes } B \xleftrightarrow{K-} A.$$

G6 说明,A 相信 B 相信 K 是适用于 A 的未经确认的密钥.注意,此处 B 的信念超出了 A 的控制范围.因此,以 A 的观点,G6 的意义在于 B 已经确认了 A 的身份,即 B 确认 A 是与 B 共享密钥 K 的主体.

注意,(G4): A believes $A \xleftrightarrow{K+} B$ 与 B 关于 K 的信念无关.因此(G4)与(G6)是不同的.此外,

$$A \text{ believes } A \xleftrightarrow{K+} B \not\equiv (A \text{ believes } A \xleftrightarrow{K-} B) \wedge (A \text{ believes } B \text{ has } K).$$

关于认证目标的进一步讨论,读者可参见文献[16,29,30].

2 BAN 类逻辑分析方法与串空间模型

2.1 SVO逻辑

SVO 逻辑吸取了 BAN 逻辑、GNY 逻辑、AT 逻辑和 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 逻辑对一些概念重新进行定义(有别于 AT 逻辑),从而取消了 AT 逻辑系统中的一些限制.

SVO 逻辑所用的记号与 BAN 类逻辑相似,其中特有的 12 个符号及其含义如下:

1. *:主体所收到的、不可识别的消息;
2. $\widetilde{K}$:密钥 K 对应的解密密钥;
3. $\{X^P\}_K$:加密消息 $\{X\}_K$,P 是发送者(常省略);
4. $[X]_K$:用密钥 K 对消息 X 签名后所得到的签名消息;
5. $\langle X_P \rangle_Y$:合成消息$\langle X \rangle_Y$,P 是发送者(常省略);
6. $PK_\psi(P,K)$:K 为主体 P 的公开加密密钥;
7. $PK_\sigma(P,K)$:K 为主体 P 的公开签名验证密钥;
8. $PK_\delta(P,K)$:K 为主体 P 的公开协商密钥(或参数);
9. $SV(X,K,Y)$:用密钥 K 可验证 X 是 Y 的签名;
10. $P \xleftrightarrow{K} Q$:K 是 P 和 Q 之间的良好共享密钥,但 P 和 Q 可能都不知道 K;
11. $P \xleftrightarrow{K-} Q$:K 是 P 的适合于与 Q 通信的非确认共享密钥;

12. $P \xleftrightarrow{K+} Q$:K 是 P 的适合于与 Q 通信的确认共享密钥.

与 AT 逻辑相似,SVO 逻辑也将语言划分为集合 T 上的消息语言 M_T 和公式语言 F_T.其中 T 为原子术语集,由主体、共享密钥、公开密钥、私有密钥及一些常量符号构成.

应用 SVO 逻辑对安全协议进行形式化分析可以分为以下 3 个步骤:

(1) 给出协议的初始化假设集 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 逻辑语言表示的一个公式集;

(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.

因此,正确理解安全协议中消息的含义和协议的设计目标,是应用 SVO 逻辑进行协议分析的基础.

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 逻辑不仅成功地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[31,32].

2.2 串空间模型与BAN类逻辑

AT 逻辑和 SVO 逻辑已经引入模型论语义,是 BAN 类逻辑发展过程中重要的一步.但是,其语义中的计算模型源于认知逻辑中对分布计算进行推理的一般模型,并不特别适用于认证协议.因此,在 BAN 类逻辑中引进串空间模型语义,是一种可行的方法[33].

串(strand)是参与协议的主体可以执行的事件序列.对于诚实的主体,该事件序列是根据协议定义,由发送事件和接收事件组合而成的.此外,该模型还定义了攻击者串,描述攻击者的行为.

串空间是由协议参与者,包括诚实主体和攻击者的串组成的串集合.串集合之间可以穿插组合,使一个串的发送消息对应另一个串的接收消息.丛(bundle)是串空间中的重要概念,表示一个完整的协议交换串空间的子集.丛可以表示为有限无环图,其中的边表示结点间的因果依赖关系.在串空间模型中,共有两种不同类型的边:

(1) $n_1 \rightarrow n_2$ 表示 n_1 发送消息 M 被 n_2 接收;

(2) $n_1 \Rightarrow n_2$ 表示 n_1 是 n_2 在同一个串上的直接因果前驱.

关于串空间模型的详细介绍,请参见文献[4,5,34].

我们假设有一个运行集 R 和一个解释 π.π 将每个命题常量 $p \in T$ 映射到一个点集 $\pi(p)$,在这些点上,p 的值为“真”.公式 φ 在点 (r,t) 为真,写作 $(r,t) \models \varphi$. $\models \varphi$ 表示 φ 有效,即 φ 在所有运行点均为真.

令 $\langle C,s,i \rangle$ 表示丛 C 中的点,亦即丛 C 中串 s 上的第 i 个结点.令 $princ(s)$ 表示执行串 s 的主体.

作为举例,以下是 SVO 逻辑中 4 个典型公式的串空间模型语义,其中 M 为任何消息.

(1) $\langle C,s,i \rangle \models P$ sent M

当且仅当 C 中存在一个结点 $\langle t,j \rangle$,满足:(a) $princ(t) = P$;(b) $\langle t,j \rangle \preceq \langle s,i \rangle$;(c) $term(\langle t,j \rangle) = +M$.

(2) $\langle C,s,i \rangle \models P$ received M

当且仅当 C 中存在一个结点 $\langle t,j \rangle$,满足:(a) $princ(t) = P$;(b) $\langle t,j \rangle \preceq \langle s,i \rangle$;(c) $term(\langle t,j \rangle) = -M$.

在给出公式 P said M 的串空间模型语义之前,我们还需要做下述准备:

设 A 是我们所讨论的项代数集合.若 $K \subseteq \hat{K}$, A 的 K 理想是 A 的子集 I,使得对所有的 $h \in I$, $g \in A$ 及 $k \in K$,均有

(i) $hg, gh \in I$;

(ii) $\{h\}_k \in I$.

我们将包含 h 的最小 K 理想记为 $I_K[h]$.

令 $K \subseteq \hat{K}$, $s \in A$ 是 $t \in A$ 的 K 子项,记为 $s \sqsubset_K t$,当且仅当 $t \in I_K[s]$.

若在定义中有 $K = \hat{K}$,则简称 s 是 t 的子项,并记为 $s \sqsubset t$.

(3) $\langle C,s,i \rangle \models P$ said M

当且仅当存在消息 M',满足 $\langle C,s,i\rangle \models P \text{ sent } M'$,且 $M \sqsubset_K M'$.这里,K 是 P 在 $\langle s,i\rangle$ 拥有的密钥集合.

为了引入公式 $P \text{ got } M$ 的串空间模型语义,我们需要过滤(filter)的定义,它是理想的对偶,亦称互理想(co-ideal).

若 $K \subseteq \hat{K}$,A 的 K 过滤是 A 的子集 F,使得对所有的 $h,g \in A$ 及 $k \in K$,均有:

(i) 若 $hg \in F$ 成立,则有 $h \in F$ 且 $g \in F$;

(ii) 若 $\{h\}_k \in F$ 成立,则有 $h \in F$ 对 $k^{-1} \in K$ 成立.

我们将包含 h 的最小 K 过滤记为 $F_K[h]$.

(4) $\langle C,s,i\rangle \models P \text{ got } M$

当且仅当存在消息 M',满足 $\langle C,s,i\rangle \models P \text{ received } M'$,且 $M \in F_K[M']$.这里,K 是 P 在 $\langle s,i\rangle$ 拥有的密钥集合.

3 安全协议的设计

3.1 安全协议设计的原则

在设计协议时,如何保证安全协议能够满足保密性、无冗余、认证身份等设计目标呢?经过总结,我们提出了以下安全协议的设计原则:

(1) 设计目标明确,无二义性;

(2) 最好应用描述协议的形式语言,对安全协议本身进行形式化描述;

(3) 通过形式化分析方法证明安全协议实现了设计目标;

(4) 安全性与具体采用的密码算法无关;

(5) 保证临时值和会话密钥等重要消息的新鲜性,防止重放攻击;

(6) 尽量采用异步认证方式,避免采用同步时钟(时戳)的认证方式;

(7) 具有抵抗常见攻击,特别是防止重放攻击的能力;

(8) 进行运行环境的风险分析,作尽可能少的初始安全假设;

(9) 实用性强,可用于各种网络的不同协议层;

(10) 尽可能减少密码运算,降低成本,扩大应用范围.

其中,第(7)条十分重要.Dolev 和 Yao 于 1983 年提出了 Dolev-Yao[11]攻击者模型.它是对攻击者的知识和能力进行概括的最早的模型,此后关于安全协议的形式化分析或多或少都受到他们的工作的影响."永远不低估攻击者的能力",这是设计安全协议时应当时刻牢记的一条重要原则.

3.2 应用形式化方法指导安全协议设计

在安全协议发展的近 20 年中,形式化方法主要用于分析安全协议.但是,形式化方法用于指导安全协议的设计同样有效.近年来,关于这方面的研究日益增多[3,35,36].

下面我们举例说明如何应用串空间模型和认证测试方法来指导安全协议的设计[36].在这个例子中,设计目标是修改 Otway-Rees 协议的安全缺陷[6,14],对它进行重新设计.首先,在协议中不再加密最初的请求,因此新协议将采用入测试方法.其次,新协议的目标是对每个主体都保证对方获得同一个会话密钥,这个目标原 Otway-Rees 协议没有达到.

新协议的形状如图 1 所示,根据新的设计目标增加了最后的请求与响应消息序列.A 对 B 的请求用 $\alpha_1 \to \beta_1$ 表示,B 对 A 的响应可在 $\beta_4 \to \alpha_2$ 上返回,因此不需要改变原协议的形状.我们要求 B 对 A 的请求用 $\beta_4 \to \alpha_2$ 表示,且 A 在 $\alpha_3 \to \beta_5$ 上对此请求进行响应.

A 必须在 α_1 生成临时值,然后由 S 在边 $\sigma_1 \Rightarrow \sigma_2$ 上进行变换,在结点 σ_2 上,这个临时值必须与会话密钥 K 同时嵌入一个加密分量 t_1^A.如此,将能向 A 认证服务器 S 生成 K.

同样,A 必须在 α_1 生成临时值,以供 B 用于证明获得 K.B 将沿 $\beta_3 \Rightarrow \beta_4$ 变换该临时值,并将它嵌入加密分量 t_2^A 后发送,以便满足 A 的第 2 次测试.这里,我们应用同一个临时值 N_a,而不是生成另一个临时值 N'_a,以节约计

算资源.

B 必须类似地在 β_2 生成临时值 N_b,被服务器沿边 $\sigma_1 \Rightarrow \sigma_2$ 进行变换,生成加密项 t_1^B. N_b 也要传送给 A,以便沿着边 $\alpha_2 \Rightarrow \alpha_3$ 进行变换.A 应用 K 生成包含 N_b 的加密分量 t_2^B.

通过以上讨论,我们可以对图 1 进行填充,所得结果如图 2 所示.我们在 $\alpha_1 \to \beta_1$ 和 $\beta_2 \to \sigma_1$ 边上引入了主体名,以便接收者知道提出请求的是哪个主体.在结点 α_2,可以完成 A 的两次入测试.因此,此时 A 收到他所需要的所有认证保证.

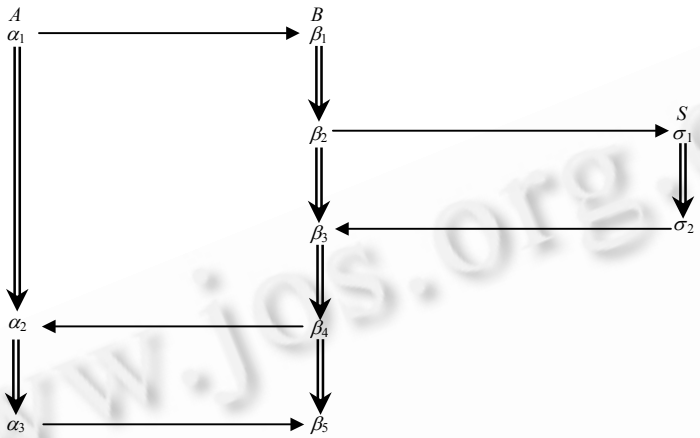

Fig.1 Shape of the new protocol expressed by strand space model

图 1 串空间模型表述的新协议形状

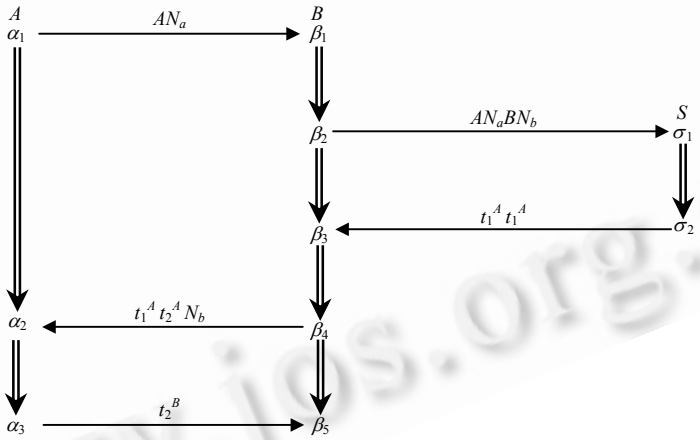

Fig.2 Important components in the new protocol

图 2 新协议中的重要分量

下面,我们定义 4 个测试分量 $t_i^A t_i^B$ $(i=1,2)$.其中,t_1^A 必须向 A 保证,S 生成 K 作为对 N_a 的响应,且 K 是 A 和 B 的会话密钥.因此,t_1^A 的形状应为 $\{..N_a BK\}_{K_A}$,其中 K_A 说明上述加密分量是由 A 生成的.类似地,t_1^B 的形状应为 $\{..N_b AK\}_{K_B}$. t_1^A 和 t_1^B 应当具有不同的形状,为此我们可以选择两个不同的正文值.例如,令 C^I 和 C^R 为常量,且 $C^I \neq C^R$,我们可以确定 t_1^A 和 t_1^B 如下:

$$t_1^A = \{C^I N_a BK\}_{K_A},\quad t_1^B = \{C^R N_b AK\}_{K_B}.$$

对于两个主体的第 2 个认证测试,我们只要求用 K 加密临时值 N_a 和 N_b,且测试分量具有不同的形状,因此我们可以定义

$$t_2^A = \{C^I N_a\}_K,\quad t_2^B = \{C^R N_b\}_K.$$

因此,新协议达到了如下目标:(1) 发起者 A 和响应者 B 从可信服务器 S 获得新鲜的会话密钥 K;(2) A 和 B

共享 K,未对任何其他主体泄露 K;(3) 每个主体都相信,对方在协议中为收到 K 均执行到协议相应的一步.关于以上论断的形式化证明从略.

4 结 论

形式化分析方法,包括简单直接的 BAN 类逻辑分析方法,不但是分析安全协议的重要工具,也是指导安全协议设计的理论基础.

我们预期,今后这一领域的热点研究方向包括:(1) 减少对协议所作的基本假设,例如,加密体制的“完善”(perfect)假设、自由加密(free encryption)假设等,使理论研究尽量接近实际.(2) 扩大协议的分析范围.例如,分析安全电子商务协议;分析协议的公平性等.(3) 增加分析“协议组合”的能力,这是目前的研究热点与难点之一.(4) 综合不同分析方法的特点,例如,CSP 模型、串空间模型、模型校验器(model checker)方法、线性逻辑方法等的相互比较与结合的研究.(5) 安全协议的自动生成与校验研究.(6) 参加协议的主体数目可以无限增加时的研究,等等.

References:

[1] Qing, SH. Cryptography and Computer Network Security. Beijing: Tsinghua University Press, 2001. 127~147 (in Chinese).

[2] Qing, SH. Formal analysis of authentication protocols. Journal of Software, 1996,7:107~114 (in Chinese with English abstract).

[3] Meadows C. Formal verification of cryptographic protocols: A survey. In: Advances in Cryptology, Asiacrypt'96 Proceedings. LNCS 1163, Berlin: Springer-Verlag, 1996, 135~150.

[4] Thayer FJ, Herzog JC, Guttman JD. Strand spaces: Why is a security protocol correct? In: Proceedings of the 1998 IEEE Symposium on Security and Privacy. Los Alamitos: IEEE Computer Society Press, 1998. 160~171.

[5] Thayer FJ, Herzog JC, Guttman JD. Strand spaces: Proving security protocols correct. Journal of Computer Security, 1999,7(2-3): 191~230.

[6] Burrows M, Abadi M, Needham R. A logic of authentication. Research Report 39, Digital Systems Research Center, 1989.

[7] Gong L, Needham R, Yahalom R. Reasoning about belief in cryptographic protocols. In: Proceedings of the 1990 IEEE Computer Society Symposium on Research in Security and Privacy. Los Alamitos: IEEE Computer Society Press, 1990. 234~248.

[8] Abadi M, Tuttle MR. A semantics for a logic of authentication. In: Proceedings of the 10th ACM Symposium on Principles of Distributed Computing. ACM Press, 1991. 201~216.

[9] van Oorschot PC. Extending cryptographic logics of belief to key agreement protocols. In: Proceedings of the 1st ACM Conference on Computer and Communications Security. ACM Press, 1993. 233~243.

[10] Syverson, PF, van Oorschot PC. On unifying some cryptographic protocol logics. In: Proceedings of the 1994 IEEE Computer Society Symposium on Research in Security and Privacy. Los Alamitos: IEEE Computer Society Press, 1994. 14~28.

[11] Dolev D, Yao A. On the security of public key protocols. IEEE Transactions on Information Theory, 1983,29(2):198~208.

[12] Syverson P. A taxonomy of replay attacks. In: Proceedings of the Computer Security Foundations Workshop. Los Alamitos: IEEE Computer Society Press, 1994. 187~191.

[13] Wang GL, Qing SH, Zhou ZF. Some new attacks upon authentication protocols. Journal of Software, 2001,12(6):907~913 (in Chinese with English abstract).

[14] Clark J, Jacob J. A survey of authentication protocol literature: Version 1.0. 1997. http://www-users.cs.york.ac.uk/~jac/under the link\Security Protocols Review.

[15] Needham R, Schroeder M. Using encryption for authentication in large networks of computers. Communications of the ACM, 1978, 21(12):993~999.

[16] Lowe G. Breaking and fixing the Needham-Schroeder public-key protocol using FDR. Software——Concepts and Tools, 1996,17: 93~102.

[17] Nessett DM. A critique of the burrows, Abadi and Needham logic. ACM Operating Systems Review, 1990,24(2):35~38.

[18] Syverson P. Knowledge, belief, and semantics in the analysis of cryptographic protocols. Journal of Computer Security, 1992,1(3): 317~334.

[19] Bieber P. A logic of communication in a hostile environment. In: Proceedings of the Computer Security Foundations Workshop III. Los Alamitos: IEEE Computer Society Press, 1990. 14~22.

[20] Syverson P. Formal semantics for logics of cryptographic protocols. In: Proceedings of the Computer Security Foundations Workshop III. Los Alamitos: IEEE Computer Society Press, 1990. 32~41.

[21] Rangan PV. An axiomatic basis of trust in distributed systems. In: Proceedings of the 1988 Symposium on Security and Privacy. Los Alamitos: IEEE Computer Society Press, 1988. 204~211.

[22] Moser L. A logic of knowledge and belief for reasoning about computer security. In: Proceedings of the Computer Security Foundations Workshop II. Los Alamitos: IEEE Computer Society Press, 1989. 57~63.

[23] Yahalom R, Klein B, Beth T. Trust relationships in secure systems: A distributed authentication perspective. In: Proceedings of the 1993 IEEE Symposium on Security and Privacy. Los Alamitos: IEEE Computer Society Press, 1993. 150~164.

[24] Kindred D. Theory generation for security protocols [Ph.D. Thesis]. Pittsburgh: Department of Computer Science, Carnegie Mellon University, 1999.

[25] CCITT. CCITT draft recommendation X.509. The directory-authentication framework, Version 7, 1987.

[26] Burrows M, Abadi M, Needham R. Rejoinder to Nessett. Operating Systems Review, 1990,24(2):39~40.

[27] Diffie W, Hellman ME. New directions in cryptography. IEEE Transactions on Information Theory, 1976,IT-22(6):644~654.

[28] Doraswamy N, Harkins D. IPSEC: The New Security Standard for the Internet, Intranets, and Virtual Private Networks. Prentice Hall, Inc., 1999.

[29] Gollmann D. What do we mean by entity authentication? In: Proceedings of the IEEE Symposium on Security and Privacy. Los Alamitos: IEEE Computer Society Press, 1996. 46~54.

[30] Lowe G. A hierarchy of authentication specifications. In: Proceedings of the 10th IEEE Computer Security Foundations Workshop. Los Alamitos: IEEE Computer Society Press, 1997. 31~43.

[31] Zhou J, Gollmann D. Towards verification of non-repudiation protocols. In: International Refinement Workshop and Formal Methods Pacific 1998. Berlin: Springer-Verlag, 1998. 370~380.

[32] Qing, SH. A new non-repudiation protocol. Journal of Software, 2000,11(10):1338~1343 (in Chinese with English abstract).

[33] Syverson PF. Towards a strand semantics for authentication logic. Electronic Notes in Theoretical Computer Science, 2000,20: 62~72.

[34] Thayer FJ, Herzog JC, Guttman JD. Strand spaces: Honest ideals on strand spaces. In: Proceedings of the 1998 IEEE Computer Security Foundations Workshop. Los Alamitos: IEEE Computer Society Press, 1998. 66~77.

[35] Heintze N, Tygar, JD. A model for secure protocols and their composition. IEEE Transactions on Software Engineering, 1996, 22(1):16~30.

[36] Guttman JD, Thayer FJ. Authentication tests. In: Proceedings of the 2000 IEEE Symposium on Security and Privacy. Los Alamitos: IEEE Computer Society Press, 2000. 150~164.

附中文参考文献:

[1] 卿斯汉.密码学与计算机网络安全.北京:清华大学出版社,2000.127~147.

[2] 卿斯汉.认证协议的形式化分析.软件学报,1996,7:107~114.

[13] 王贵林.卿斯汉,周展飞.认证协议的一些新攻击方法.软件学报,2001,12(6):907~913.

[32] 卿斯汉.一种新型的非否认协议.软件学报,2000,11(10):1338~1343.