ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.20, No.11, November 2009, pp.3060−3076
doi: 10.3724/SP.J.1001.2009.03392

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

密码协议分析的信任多集方法*

董 玲+, 陈克非, 来学嘉

(上海交通大学 计算机科学与工程系,上海 200240)

Belief Multiset Formalism for Cryptographic Protocol Analysis

DONG Ling+, CHEN Ke-Fei, LAI Xue-Jia

(Department of Computer Science and Engineering, Shanghai Jiaotong University, Shanghai 200240, China)

+ Corresponding author: E-mail: ldong@sh163c.sta.net.cn

Dong L, Chen KF, Lai XJ. Belief multiset formalism for cryptographic protocol analysis. *Journal of Software*, 2009,20(11):3060−3076. http://www.jos.org.cn/1000-9825/3392.htm

Abstract: This paper proposes a belief multisets formalism for analyzing cryptographic protocols, and the formalism is foundationally different from the previous: a participant's beliefs should depend only on the sent or received fresh messages and the beliefs already possessed by this party. The presented security adequacy of unilateral authentication secure, mutual authentication secure, unilateral session key secure, or mutual session key secure is proved not only substantial but also necessary to meet 4 security definitions respectively under the computational model of matching conversation and indistinguishability. Illustrations and comparison show that the analysis results based on the belief multisets suggest the correctness of a protocol or the way to construct attacks intuitively from the absence of security properties. The formalism is independent of the concrete formalization of a protocol or attackers' possible behaviors. The formalism can be developed not only by hand but also by automation.
Key words: cryptographic protocol; security analysis; formalism; automation

摘 要: 提出了一种基于逻辑的信任多集方法,它与已有的密码协议安全性分析方法本质上不同:每个参与主体建立的新信任只应依赖于该主体已拥有的信任和接收或发送的包含了信任的新鲜性标识符的消息本身.在基于匹配对话和不可区分性的计算模型下,证明了给出的保证密码协议单方认证安全、双方认证安全、单方密钥安全和双方密钥安全的充分必要条件分别满足4个可证安全定义.实例研究和对比分析表明,信任多集方法有以下特点:首先,安全性分析结果要么证明了一个密码协议是安全的,要么指出了密码协议安全属性的缺失,由安全属性的缺失能够直接导出构造攻击的结构;其次,分析方法与密码协议和攻击者能力的具体形式化描述无关;最后,不仅可用于手工分析,而且便于开发出自动验证系统.
关键词: 密码协议;安全性分析;形式化方法;自动化
中图法分类号: TP309 **文献标识码**: A

* Supported by the National Natural Science Foundation of China under Grant No.90704004 (国家自然科学基金); the National High-Tech Research and Development Plan of China under Grant Nos.2006AA01Z422, 2009AA01Z418 (国家高技术研究发展计划(863))

Received 2008-01-31; Revised 2008-04-02; Accepted 2008-05-19

密码协议也称为安全协议,是建立在密码体制基础上的交互通信协议,为在开放的网络环境中传送的各种信息提供认证性、保密性、完整性和不可否认性.然而,密码协议的设计非常微妙,许多密码协议在公布甚至实际应用多年之后才被发现存在漏洞[1−4].在过去的 20 多年中,研究人员提出了许多严格的形式化分析方法用于密码协议安全性的分析[4−14].目前,研究比较广泛和深入的形式化方法主要有以下几类:基于逻辑推理的分析方法、基于计算模型的分析方法、基于模型检验的分析方法和基于定理证明的分析方法.基于逻辑推理的分析方法以BAN类逻辑为代表[4].作为一种形式化分析工具,BAN类逻辑成功地找出了许多认证协议中的安全缺陷,但BAN逻辑的消息含义规则中没有有效区分消息是否新鲜的内容,造成其他主体可以发送这些消息的备份,且协议的理想化过程也是非标准的,导致BAN逻辑证明正确的协议仍可能存在漏洞.计算模型下可证明安全的思想用数学方法分析密码协议,在某种程度上要求协议设计者和分析者采取正确的或者更精确的密码学服务,它可以应用于密码协议的安全性证明[6−8].基于模型检验的分析方法从协议的初始状态开始对合法主体和一个攻击者所有可能的执行路径进行穷尽搜索,以期找到协议可能存在的错误[9,10].实验表明,这个方法是有效的.该方法存在的主要问题是,如何将协议说明成有限状态系统而又不增加或减少协议的安全性.基于定理证明的分析方法中,最著名的是Strand Space和认证测试的方法[11−13].Strand Space是一种非常有效的密码协议形式化分析方法,但是分析过程与密码协议的形式化和攻击者能力的具体形式化密切相关,而攻击者可能的行为方式是不断发展变化的.

已有的形式化分析方法取得了有目共睹的成绩,但是仍有许多重要问题没有得到满意的解决,其中最为重要的一个问题就是,密码协议足够安全的量化指标是什么,以及如何建立密码协议的安全性.如Ran Canetti和Hugo Krawczyk在著名的CK模型中提出了认证转换以保证密码协议足够安全[11],但对于如何对密码协议的安全性进行精确的量化以及如何分析已知协议的安全性,未能给出明确的方法.另一个要研究的问题是,提出一种简单的适于应用的形式化方法来具体量化密码协议的安全性,用于密码协议的安全性分析与设计.

基于逻辑推理、定理证明思想,本文提出一种信任多集密码协议形式化分析方法,并在计算模型下给出了相关的安全性证明.信任多集形式化方法的核心思想是,对每个通信参与主体而言，密码协议的安全性取决于发送或者接收的、包含自身已相信新鲜的新鲜性标识符的单向变换..

基于匹配对话[7,8]的认证性和不可区分性[6]的保密性,我们给出单方认证安全、双方认证安全、单方密钥安全和双方密钥安全 4 种可证安全定义,以满足不同的安全需求.在给定密码协议安全性定义和信任多集方法详细语义说明的基础上,提出保证认证密码协议足够安全的充分必要条件,并证明这些量化安全指标在计算模型下分别满足 4 个可证安全定义.最后,以Needham-Schroeder公钥认证协议、传感器网络环境下基于Kerberos的对密钥管理方案为例,说明如何应用信任多集方法分析协议的安全属性,并将该方法与已有的形式化方法进行对比分析.实例研究和对比分析结果表明,信任多集方法不仅是证明密码协议正确性的方法,而且是查找协议错误的方法.也就是说,首先,信任多集方法给出的保证认证密码协议足够安全的安全属性量化指标不仅是充分的,而且是必要的;其次,对于存在安全属性缺失的密码协议,信任多集方法的分析结果直接指明了构造攻击的结构;再次,信任多集方法与密码协议的具体形式化无关,与攻击者能力的具体形式化无关;最后,信任多集方法具有清晰的语义和统一的密码协议分析模型,不仅可用于手工分析而且便于开发出自动验证系统.

1 基本概念和安全性定义

1.1 基本概念和初始假设

主体是指通信的合法参与者,是概率多项式时间机器,主体间通过点到点链路互相交换消息.消息是指通信过程中在网络上传输的数据.协议是指在两方或互相协作的多方之间进行通信的过程.消息驱动协议是指某一方触发一次消息请求,随后两方或互相协作的多方之间按照约定处理接收的消息,生成并返回消息给另一方,等待新消息的到来.消息驱动协议是当前网络通信中最为常见的形式,具有异步的特征.一个主体可以同时运行多个协议或一个协议的多个实例,每一个协议的运行实例称为一个会话.

新鲜性是协议中的对话具有的一种属性,当一个标识符或者一条消息能够被确认是为该次协议运行所特

别产生的,即为新鲜的.例如,一个标识符或者一条消息是由某主体专门为这次协议生成的,或者是与这个特别生成的内容在一个单向变换后传输的,且该合成消息涉及了响应者所对应的密码操作,那么这个主体就可以确认这个标识符或者这条消息具有新鲜性.新鲜性标识符是指为协议的某次运行产生的一个唯一的标识符,可以是随机数、时间戳、新会话密钥,或生成新会话密钥的组成部分.信任的新鲜性标识符是指协议中的某个合法参与者相信新鲜的新鲜性标识符,可以是该主体为本次会话生成的新鲜性标识符,或者该主体相信是其他主体为本次会话生成的新鲜性标识符.对于不同的参与者和不同的协议运行,信任的新鲜性标识符是不同的.新鲜性消息是指包含信任的新鲜性标识符的消息.主体的活现性是指协议中的一个合法参与者相信交互的另一方的确参与了协议的本次运行.新鲜性标识符的保密性是指协议中的某个合法参与者相信该标识符是以攻击者不可知的密文方式传送的,即保密的.特别需要指出的是,用私钥签名的新鲜性标识符不是保密的.新鲜性标识符的新鲜性是指协议中的某个合法参与者相信该标识符是本次协议运行中新产生的,而不是一个旧的会话值.新鲜性标识符的关联性是指协议中的某个合法参与者相信这个新鲜性标识符是与本次协议运行的主体相关联的,而不可能与其他主体关联.

定义 1(术语). 协议参与者可能交换的新鲜性消息称为术语 $\hat{m}$, 一个协议中所有参与者间可能交换的术语集合记为 $\hat{M}$.术语可递归定义如下:

(1) 若 $\hat{m}$ 是信任的新鲜性标识符,则 $\hat{m}$ 是术语.

(2) 若 $\hat{m}$ 是术语,o 是主体身份或者其他新鲜性标识符,则 $\{\hat{m},o\}$ 或 $\{o,\hat{m}\}$ 也是术语(表示将 $\hat{m}$ 和 o 进行连接).

(3) 若 $\hat{m}$ 是术语,k是密钥(对称密钥、非对称密钥等),则$\{m\}_k$是术语(表示将 $\hat{m}$ 用k加密);若 $\hat{m}$ 是术语,o是主体身份或某个确定的标识符,则 $\{o\}_{\hat{m}}$ 也是术语(表示将o用 $\hat{m}$ 加密).

定义 2(符号术语). 一个符号术语是一个二元组 $(\delta,\hat{m})$, 其中,δ是一个符号, $\hat{m}\in\hat{M}$, 一个符号术语写为 $+\hat{m}$ 或 $-\hat{m}$. $+\hat{m}$ 和 $-\hat{m}$ 分别表示发送的新鲜性消息和接收的新鲜性消息.

“对话”[7]是通信参与者发送出(接收到)的一系列时序消息系列以及因此接收到(和发送出)的应答.令 $\tau_1<\tau_2<\ldots<\tau_n$为参与主体在其会话时记录的一个时间序列.对话可以由下列序列表示:

$$conv=(\tau_1,\hat{m}_1,\hat{m}_1'),(\tau_2,\hat{m}_2,\hat{m}_2'),\ldots,(\tau_n,\hat{m}_n,\hat{m}_n').$$

其中, $\hat{m}_1,\hat{m}_1',\hat{m}_2,\hat{m}_2',\ldots,\hat{m}_n,\hat{m}_n'\in\hat{M}$.

这个序列表明:在时间τ_1,用 $\hat{m}_1$ 提问,应答是 $\hat{m}_1'$;在随后的时间 $\tau_2>\tau_1$,用 $\hat{m}_2$ 提问,应答是 $\hat{m}_2'$;一直继续到时间 τ_n,用 $\hat{m}_n$ 提问,应答是 $\hat{m}_n'$.如果 $\hat{m}_1$=“”,那么该通信参与者为通信发起者;如果 $\hat{m}_n'$=“无消息输出”,那么该通信参与者结束了本次通信会话.如果对话中用省略号表示,则说明该对话的拥有者不关心这条接收到(和发送出)的消息内容(如明文),这条消息对匹配对话没有影响.协议运行结束,通信参与者对意定通信伙伴所声称的身份有 3 种处理结果:接受、拒绝、无法判别.“拒绝”、“接受”判定随时可能作出,而“无法判别”判定,协议运行结束才作出.

下面给出一些初始假设.(1) 本文不考虑对底层密码算法本身的攻击,这也是目前密码协议分析方法大都遵从的密码协议建模和分析原则.也就是说,密码协议不安全,不是因为该协议所采用的特定底层密码算法不安全,而是因为协议设计上的缺陷.这些缺陷使得攻击者能够在不需要破解底层密码算法的条件下就可以破坏密码协议的安全性目标.(2) 对于采用非对称密码技术的机制(或者对称密码技术的机制),假设密码协议参与者在协议运行前已经获得了自身的私钥和其他参与者的公钥(或者与通信对方或可信第三方的长期共享密钥).(3) 假设协议参与者能够保证自身为协议的某次运行产生的新鲜性标识符具有唯一性和新鲜性.(4) 假设攻击者是概率多项式时间机器,运行在Dolev-Yao多协议并行执行环境[14]中,攻击者对通信链路具有完全的控制能力.此外,攻击者还能进行密码课程训练.这些课程帮助攻击者在解密模式下获得有条件的优势,本文中,我们仍称这类攻击者为Dolev-Yao模型下的攻击者.(5) 假设协议中任意两条消息能提取的最大术语不同.最大术语是指对同一条消息重复定义 1 的步骤(2)、步骤(3)所能形成的术语.

1.2 安全性定义

1993 年,Bellare和Rogaway提出了基于匹配对话的认证性安全性定义[7,8].由于攻击者对通信链路具有完全的控制能力,本文假定合法主体之间的所有通信都是经过攻击者的,即所有通信在攻击者和某一个合法参与者之间进行,除非在时间τ_n,参与者作出了接受这个对话的判定.假设A,B进行了一次协议运行,A有对话,

$$conv=(\tau_0,\text{“”},m_1),(\tau_2,m_1',m_2),(\tau_4,m_2',m_3),...,(\tau_{2t-2},m_{t-1}',m_t).$$

如果存在时间序列$\tau_1<\tau_2<\ldots<\tau_n$和$conv'=(\tau_1,m_1,m_1'),(\tau_3,m_2,m_2'),(\tau_5,m_3,m_3'),...,(\tau_{2t-1},m_t,m_t')$,其中$m_t'$=“无消息输出”,则称$conv$在意定的通信方$B$存在匹配的对话$conv'$,即在参与者$A$看来这两个对话就是匹配对话[7].

如果无论何时通信双方完成一次协议运行,某一个通信参与者都相信记录的 $conv$ 在意定的通信方总存在匹配的对话$conv'$,认证协议在这个通信参与者的角度就是安全的.攻击者攻破了目标认证协议是指对话$conv$在意定的通信方没有匹配对话 $conv'$,参与者仍然接受了意定通信方的身份.要指出的是,本文中需要匹配的只是新鲜性消息即术语,而忽略其他提问和应答的消息,如仅起提示作用的明文等.

1984 年,Goldwasser和Micali提出了基于不可区分性的保密性安全性定义[6]:凡是在给定密文条件下可以有效计算的明文信息,都可以在没有该密文的条件下有效地计算.攻击者攻破目标密码协议是指在不知道密文对应的密钥和没有破解底层密码算法的条件下,在密码协议运行中,攻击者仍然能够获得一些有关相应明文的信息.这里,获得是指能够有效区分协议中加密内容的值(如新会话密钥或新会话密钥的组成部分)和一个随机值.

类似于文献[11]中定义的 KE-Adversary,我们基于 Dolev-Yao 模型下的任意攻击者 I 进行安全性定义和分析,并允许 I 进行加、解密的密码课程训练.

单方认证安全是指在协议的某次运行中,参与通信的某一方实体确认另一方实体的身份.典型的应用是电子表决中,选民需要向选票中心证明自己的身份,但要匿名表决.另一种情况是用户向服务器证明身份以获得相应的服务资源,或者服务器向用户证明自己的身份,以表明所提供的信息的确来自所声明的服务器.基于匹配对话给出单方认证安全的定义.给定任意一对通信者 A 和 B,A 和 B 之间共享一个大小为 $\mathcal{N}$的长期对称密钥(或者 A 和 B 各有一个私钥以及包括攻击者在内的所有参与者都知道的公钥).参与者 A 试图在一次会话中认证参与者 B.这种尝试可能是由 A 发起的,也可能是对意定的通信者 B 发送的某个消息的应答.

定义 3(单方认证安全(UA-安全)). π是以认证性为目标的密码协议.假定存在 Dolev-Yao 模型下的攻击者 I,如果攻击者 I 不能以一个不可忽略概率成功,那么主体 A 可以相信密码协议π是 UA-安全的.这里,成功是指 A 接受意定通信另一方主体 B 的身份,但在 B 中没有与 A 记录的对话相匹配的对话.

双方认证安全是指在协议的某次运行中,参与通信的双方实体互相确认对方实体的身份.MA-安全的应用很多,包括需要双方身份认证的电子选举、提供资源共享的客户服务器方式身份认证等.类似于定义 3,基于匹配对话给出双方认证安全定义.

定义 4(双方认证安全(MA-安全)). π是以认证性为目标的密码协议.假定存在 Dolev-Yao 模型下的攻击者 I,如果攻击者 I 不能以一个不可忽略概率成功,密码协议π就是 MA-安全的.这里,成功是指通信某一方接受了通信另一方的身份,而通信另一方没有匹配对话.

单方密钥安全是指在协议的某次运行中,参与通信的某一方认证另一方的身份,并相信由被认证的一方为本次运行产生的新会话密钥能够在不安全的网络环境中为敏感数据提供一个安全的通信信道.例如客户服务器方式,客户一方 A 对服务器一方 B 进行单方密钥安全的认证,或反之.类似于文献[11],我们和攻击者进行一个游戏:投掷一枚硬币 $b, b\xleftarrow{R}\{0,1\}$,由攻击者猜测是正面($b$=0)还是反面($b$=1).当 b=0 时,提供攻击者新的会话密钥 k;否则,从新的会话密钥 k 的概率分布中随机选取一个值 r 提供给攻击者 I.攻击者 I 给出对 b 的猜测 b'.

定义 5(单方密钥安全(UK-安全)). π是以认证性和保密性为目标的密码协议.假定存在 Dolev-Yao 模型下的攻击者 I,但是密码协议π仍满足下列条件,那么主体 A 可以相信密码协议π是 UK-安全的:

(1) 如果通信一方 A 认为已经与意定的另一方 B 完成了一次协议的运行,那么 A 相信未被攻破的、声明为通信方 B 的主体一定对同一会话进行了响应,并为本次会话输出了与 A 相同的会话密钥 k;

(2) 攻击者正确猜测 b 的概率不大于 1/2 加一个可忽略量.

双方密钥安全是指在协议的某次运行中,参与通信的双方互相认证对方的身份,并由其中一个主体或者两个主体共同生成一个新的会话密钥.通信的双方都相信新会话密钥能够在不安全的网络环境中为敏感数据提供一个安全的通信信道.基于匹配对话的认证性和不可区分性的保密性,给出 MK-安全定义,即文献[11]中的 SK-secure 定义.我们和攻击者进行定义 5 中同样的游戏.

定义 6(双方密钥安全(MK-安全)(SK-secure[11])). π是以认证性和保密性为目标的密码协议.假定存在Dolev-Yao模型下的攻击者I,但是密码协议π仍满足下列条件,那么密码协议π是MK-安全的:

(1) 如果未被攻破的通信双方完成了同一会话,那么双方将输出相同的会话密钥;

(2) 攻击者正确猜测 b 的概率不大于 1/2 加一个可忽略量.

2 信任多集形式化方法

2.1 定义与描述

在信任多集形式化方法中,密码协议的安全属性是指参与通信的某一方拥有的关于该密码协议安全性的信任,包括主体元素的信任和新鲜性标识符元素的信任.从不同的协议参与者角度出发,密码协议的安全属性是不同的.允许集合中的元素重复,允许元素具有不同的属性,这是我们使用多集而不是集合的主要原因.例如,用于认证性目标的主体元素仅有活现性属性新鲜性标识符元素有保密性、新鲜性和关联性属性.信任多集是指在协议的某次运行中,从某个合法参与者的角度出发,建立的关于该密码协议安全性的信任即安全属性的集合.同一参与者的同次协议运行拥有相同的信任多集,同一参与者的不同次协议运行拥有不同的信任多集,同次协议运行的不同参与者也拥有不同的信任多集.我们用$b_{\rho,t}$表示某个主体ρ在时刻t拥有的信任多集,即主体ρ在时刻t建立的关于多集元素(如,主体元素p_i、新鲜性标识符元素N或N'等)的信任的集合,表示为

$$\lfloor\langle\ldots N\ldots\rangle,\langle\ldots N'\ldots\rangle,\ldots,\langle\ldots p_i\rangle\rfloor.$$

为叙述方便,下面给出信任多集方法的一些符号说明.

ρ	任意主体,是密码协议运行的参与者.
p_i或p_j	由下标标注的主体,是协议的某次运行中特定的参与者.
S	密码协议通信中的可信第三方.
t	任意时间点,不是时间段.
$t_1,t_2,\ldots,t_\$$	分别表示协议运行之前,执行完第 1 条消息的发送和接收,...,协议运行结束等时间点.
N或N'	任意的新鲜性标识符,可以是随机数、时间戳、新会话密钥、生成新会话密钥的组成部分等.如果一个新鲜性标识符是第一次出现在协议中,那么该新鲜性标识符是发送主体自己生成的.
N_{p_i}	由下标标注的新鲜性标识符,此处表示主体p_i生成的新鲜性标识符.
k	密码体制中的加密密钥;k^{-1},对应k的解密密钥.在对称密码体制中,k和k^{-1}是相等的.
k_{ij}	主体p_i与p_j共享的长期会话密钥.
k_i及 k_i^{-1}	在非对称密码体制中,由下标标注的主体p_i拥有的公钥k_i和私钥 k_i^{-1}.
$\Rightarrow\{\ldots N,N'\ldots\}_k$	片段某主体p_i相信新鲜性标识符N'与信任的新鲜性标识符N绑定在相同的会话中.
$\prec\{N,p_j\}$, $\prec\{N,p_i,p_j\}$	期望,$\prec\{N,p_j\}$ 表示某主体期望只有意定的通信参与方p_j能够得到自己信任的新鲜性标识符N;$\prec\{N,p_i,p_j\}$ 表示某主体p_i期望只有意定的通信参与方p_j能够得到自己信任的新鲜性标识符N,并知道N是与p_i的会话有关的.
$key(\rho,k)$	主体ρ知道密钥 k.
$\langle\ldots\rho\rangle$	关于主体ρ 的活现性的信任,缺省状态为$\langle\ldots\rho\rangle$.$\langle 1\rho\rangle$表示拥有该信任的主体相信另一个

	主体ρ参与了协议的本次运行.遵循信任多集中并的多集运算规则$\langle\ldots\rho\rangle\cup\langle 1\rho\rangle=\langle 1\rho\rangle$.
$\langle\ldots_1\ldots_2N\ldots_3\rangle$	关于新鲜性标识符 N 的信任,缺省状态为$\langle\ldots N\ldots\rangle$. "$\ldots_1$"表示新鲜性标识符元素的保密属性,"$\ldots_2$"表示新鲜性标识符元素的新鲜性属性,"$\ldots_3$"表示新鲜性标识符元素的关联属性. $\langle 1\ldots N\ldots\rangle$表示拥有该信任的主体相信 N 是保密的;$\langle 0\ldots N\ldots\rangle$表示拥有该信任的主体相信 N 是不保密的;遵循信任多集中交的多集运算规则$\langle 1\ldots N\ldots\rangle\cap\langle 0\ldots N\ldots\rangle=\langle 0\ldots N\ldots\rangle$. $\langle\ldots 1N\ldots\rangle$表示拥有该信任的主体相信 N 是新鲜的或者是长期密钥,即 N 是为本次运行新生成的值或者是长期密钥值;$\langle\ldots N\ldots\rangle$表示 N 的新鲜性无法判断,可能是旧的甚至已经泄漏的值;遵循信任多集中并的多集运算规则$\langle\ldots 1N\ldots\rangle\cup\langle\ldots N\ldots\rangle=\langle\ldots 1N\ldots\rangle$. $\langle\ldots N\ldots\rangle$表示$N$没有与任何主体关联,从而无法与协议的其他运行实例中的新鲜性标识符元素区分;用主体的名字替换"$\ldots_3$",表示该新鲜性标识符是与某运行实例相关的,主体的名字所对应的实体是该运行实例的参与者,该属性允许有多个协议参与者的名字,例如$\langle\ldots 1Np_ip_j\rangle$. 当$N$为密钥时,表示只有"$\ldots_3$"指出的主体知道该密钥,例如$\langle 11K_{ab}AB\rangle$.关联属性遵循信任多集中和的多集运算规则$\langle\ldots NA\rangle+\langle\ldots NB\rangle=\langle\ldots NAB\rangle$. 为简洁起见,信任多集中将关于保密性、新鲜性和关联性的 3 个断言联合起来表示,例如$\langle 01N\ldots\rangle$,$\langle\ldots 1Np_i\rangle$,$\langle 11Np_ip_j\rangle$.
$B_{\rho,t}\Gamma$	在时刻t,主体ρ相信断言Γ满足.例如,$B_{\rho_i,t_2}(\langle 11k_{ij}p_ip_j\rangle)$表示在时刻$t_2$,主体$p_i$相信断言$\langle 11k_{ij}p_ip_j\rangle$满足,即$k_{ij}$是保密的、新鲜的,且只有主体$p_i$,$p_j$知道$k_{ij}$.又如,$B_{A,t_0}(\neg key(I,k_b^{-1}))$表示在时刻$t_0$,主体$A$相信断言$\neg key(I,k_b^{-1})$满足,即$p_i$相信攻击者$I$不知道主体$B$的私钥$k_b^{-1}$.

2.2 推导的规则

假定ϕ和ψ均为公式,信任多集形式化方法遵循以下形式的推演规则:

R1: 如果$\vdash\phi$和$\vdash\phi\rightarrow\psi$,那么$\vdash\psi$.

R2: 如果$\vdash\phi$,那么$B_{\rho,t}\phi$.

$\vdash\phi$表示ϕ是一个重言式,即公式ϕ始终为真.例如,ϕ可能是一个完全由公理推导得到的定理.R1 规则是分离规则,如果ϕ为真,而且$\phi\rightarrow\psi$为真,那么可以推出ψ也为真.R2 规则是全称概括规则,如果ϕ始终为真,那么主体ρ在任何时间 t 都可以相信ϕ为真.

假定m_A和m_B分别是一个信任多集,o为多集中的一个元素,可以是协议运行的参与者主体元素,也可以是协议运行中的新鲜性标识符元素,那么信任多集形式化方法的并$m_{A\cup B}(o)$、交$m_{A\cap B}(o)$和$m_{A+B}(o)$运算遵循以下的多集运算规则:

R3: $m_{A\cup B}(o)=m_A(o)\cup m_B(o)$.

R4: $m_{A\cap B}(o)=m_A(o)\cap m_B(o)$.

R5: $m_{A+B}(o)=m_A(o)+m_B(o)$.

R3 规则是并的规则,表示将多集$m_A(o)$和$m_B(o)$中元素o具有的属性进行并运算,典型的应用是主体的活现性和新鲜性标识符的新鲜性属性运算.R4 规则是交的规则,表示将多集$m_A(o)$和$m_B(o)$元素o具有的属性进行交运算,典型的应用是新鲜性标识符的保密性属性运算.R5 规则是合并规则,表示将多集$m_A(o)$和$m_B(o)$元素o具有的属性加起来,典型的应用是新鲜性标识符的关联性属性运算.

2.3 公 理

公理是指在逻辑系统中永真的公式.在信任多集形式化方法中,公理包括经典谓词逻辑中的公理以及在对

称密钥和非对称密钥的密码通信体制中一些公认的假定.以下的所有规则都是关于主体p_i拥有的信任.

A0(生成规则). $+\{...N_{p_i}...\} \to B_{p_i,t}(\langle ...1N_{p_i}...\rangle)$.

生成规则A0 表示:如果参与主体p_i生成了新鲜性标识符N_{p_i},那么p_i相信新鲜性标识符N_{p_i}是新鲜的,即$B_{p_i,t}(\langle ...1N_{p_i}...\rangle)$.如果新鲜性标识符$N$出现在$p_i$发送的消息中,而且从来没有出现在任何消息中,那么$p_i$知道新鲜性标识符$N$是自己生成的$N_{p_i}$.

A1(片段规则).

(a) $-\{...N,N'...\}_{k_{ij}} \wedge B_{p_i,t}(\langle 1 1 k_{ij} p_i p_j\rangle) \wedge B_{p_i,t}(\langle ...1N...\rangle) \to B_{p_i,t}(\Rightarrow \{...N,N'...\}_{k_{ij}})$

(b) $-\{...N,N',p_j...\}_{k_{is}} \wedge B_{p_i,t}(\langle 1 1 k_{is} p_i s\rangle) \wedge B_{p_i,t}(\langle ...1N...\rangle) \to B_{p_i,t}(\Rightarrow \{...N,N'...\}_{k_{is}})$

(c) $-\{...N,N'...\}_{k_i} \wedge B_{p_i,t}(\langle 0 1 k_i p\rangle) \wedge B_{p_i,t}(\langle 1 1 k_i^{-1} p_i\rangle) \wedge B_{p_i,t}(\langle ...1N\rangle) \to B_{p_i,t}(\Rightarrow \{...N,N'...\}_{k_i})$

(d) $-\{...N,N'...\}_{k_j^{-1}} \wedge B_{p_i,t}(\langle 0 1 k_j p\rangle) \wedge B_{p_i,t}(\langle 1 1 k_j^{-1} p_j\rangle) \wedge B_{p_i,t}(\langle ...1Np_i...\rangle) \to B_{p_i,t}(\Rightarrow \{...N,N'...\}_{k_j^{-1}})$

(e) $+\{...N,N'...\}_{k_{ij}} \wedge B_{p_i,t}(\langle 1 1 k_{ij} p_i p_j\rangle) \wedge B_{p_i,t}(\langle ...1N...\rangle) \to B_{p_i,t}(\Rightarrow \{...N,N'...\}_{k_{ij}})$

(f) $+\{...N,N',p_j...\}_{k_{is}} \wedge B_{p_i,t}(\langle 1 1 k_{is} p_i s\rangle) \wedge B_{p_i,t}(\langle ...1N...\rangle) \to B_{p_i,t}(\Rightarrow \{...N,N'...\}_{k_{is}})$

(g) $+\{...N,N'...\}_{k_j} \wedge B_{p_i,t}(\langle 0 1 k_j p\rangle) \wedge B_{p_i,t}(\langle 1 1 k_j^{-1} p_j\rangle) \wedge B_{p_i,t}(\langle ...1Np_i...\rangle) \to B_{p_i,t}(\Rightarrow \{...N,N'...\}_{k_j})$

(h) $+\{...N,N'...\}_{k_i^{-1}} \wedge B_{p_i,t}(\langle 0 1 k_i p\rangle) \wedge B_{p_i,t}(\langle 1 1 k_i^{-1} p_i\rangle) \wedge B_{p_i,t}(\langle ...1N...\rangle) \to B_{p_i,t}(\Rightarrow \{...N,N'...\}_{k_i^{-1}})$

片段规则A1(a)~A1(h)表明,参与主体p_i断定新鲜性标识符N'与信任的新鲜性标识符N绑定在相同的会话中.

规则A1(a)和A1(b)表示:主体p_i收到了包含信任的新鲜性标识符N的术语$-\{...N,N'...\}_{k_{ij}}$或者$-\{...N,N',p_j...\}_{k_{is}}$,又由于$p_i$相信$k_{ij}$是$p_i$与主体$p_j$的长期共享密钥,$k_{is}$是$p_i$与可信第三方$S$的长期共享密钥且在术语中明确指明了$N$和$p_j$的通信有关,从而$N'$也是为$p_i$和$p_j$与$N$有关的特定会话而产生的,即$N'$与$N$绑定在相同的会话中.

规则A1(c)表示:主体p_i收到了包含信任的新鲜性标识符N的术语$-\{...N,N'...\}_{k_i}$,只有p_i拥有该术语的解密密钥——p_i的私钥,所以p_i断定N'是为p_i与N有关的特定会话而产生的,即N'与信任的新鲜性标识符N绑定在相同会话中.

规则A1(d)表示:主体p_i收到了包含信任的新鲜性标识符N的术语$-\{...N,N'...\}_{k_j^{-1}}$,又$k_j^{-1}$是主体$p_j$的私钥,所以$p_i$断定只能是意定的通信方$p_j$发送了这个新鲜性消息,又由于$N$与$p_i$关联,从而$N'$也是为$p_i$和$p_j$与$N$有关的特定会话而产生的,即$N'$与信任的新鲜性标识符$N$绑定在相同的会话中.

规则A1(e)和A1(f)表示:主体p_i发送了包含信任的新鲜性标识符N的术语$+\{...N,N'...\}_{k_{ij}}$或者$+\{...N,N',p_j...\}_{k_{is}}$,又由于$p_i$相信$k_{ij}$是$p_i$与主体$p_j$的长期共享密钥,$k_{is}$是$p_i$与可信第三方$S$的长期共享密钥且在术语中明确指明了$N$和$p_j$的通信有关,从而$N'$也是为$p_i$和$p_j$与$N$有关的特定会话而产生的,即$N'$与$N$绑定在相同的会话中.

规则A1(g)表示:主体p_i发送了包含信任的新鲜性标识符N的术语$+\{...N,N'...\}_{k_j}$,只有主体p_j拥有该术语的解密密钥——p_j的私钥,又由于N与p_i关联,所以p_i能够断定N'是为p_i和p_j与N有关的特定会话而产生的,即N'与信任的新鲜性标识符N绑定在相同的会话中.

规则A1(h)表示:主体p_i发送了包含信任的新鲜性标识符N的术语$+\{...N,N'...\}_{k_i^{-1}}$,该术语由$p_i$使用私钥签名得到,所以$p_i$断定$N'$与$N$绑定在相同的会话中.

A2(期望规则).

(a) $+\{...N...\}_{k_{ij}} \wedge B_{p_i,t}(\langle 1 1 k_{ij} p_i p_j\rangle) \wedge B_{p_i,t}(\langle 1 1 N...\rangle) \to B_{p_i,t}(\prec \{N,p_i,p_j\})$

(b) $+\{...N...\}_{k_j} \wedge B_{p_i,t}(\langle 1 1 k_j^{-1} p_j\rangle) \wedge B_{p_i,t}(\langle 1 1 N...\rangle) \to B_{p_i,t}(\prec \{N,p_j\})$

(c) $+\{...p_i,N...\}_{k_j}\wedge B_{p_i,t}(\langle 1 1 k_j^{-1} p_j\rangle)\wedge B_{p_i,t}(\langle 1 1 N...\rangle)\rightarrow B_{p_i,t}(\prec\{N,p_i,p_j\})$

期望规则A2(a)表示:主体p_i发送了包含信任的新鲜性标识符N的术语$+\{...N...\}_{k_{ij}}$,又由于p_i相信k_{ij}是p_i与主体p_j的长期共享密钥,所以p_i期望只有意定的通信参与方p_j才能使用k_{ij}得到新鲜性标识符N,并知道N是与p_i的会话有关的.

期望规则A2(b)表示:某主体发送了包含信任的新鲜性标识符N的术语$+\{...N...\}_{k_j}$,相信只有主体p_j拥有该术语的解密密钥——p_j的私钥,所以该主体期望只有意定的通信参与方p_j才能使用私钥k_j^{-1}得到新鲜性标识符N.

期望规则A2(c)表示:主体p_i发送了包含信任的新鲜性标识符N的术语$+\{...p_i,N...\}_{k_j}$,又由于p_i相信只有主体p_j拥有该术语的解密密钥——p_j的私钥,所以p_i期望只有意定的通信参与方p_j才能使用私钥k_j^{-1}得到新鲜性标识符N,并相信N是与p_i的会话有关的.

A3(保密性规则).

(a) $-\{...m...\}_k\wedge B_{p_i,t}(\neg key(I,k^{-1}))\wedge B_{p_i,t}(\langle 1 1 k^{-1}...\rangle)\rightarrow B_{p_i,t}(\langle 1...m...\rangle)$

(b) $+\{...m...\}_k\wedge B_{p_i,t}(\neg key(I,k^{-1}))\wedge B_{p_i,t}(\langle 1 1 k^{-1}...\rangle)\rightarrow B_{p_i,t}(\langle 1...m...\rangle)$

(c) $-\{...m...\}_k\wedge B_{p_i,t}(key(I,k^{-1}))\rightarrow B_{p_i,t}(\langle 0...m...\rangle)$

(d) $+\{...m...\}_k\wedge B_{p_i,t}(key(I,k^{-1}))\rightarrow B_{p_i,t}(\langle 0...m...\rangle)$

保密性规则A3(a),A3(b)表明:若消息m是保密的,那么m一定是以密文方式传送的,且密文对应的解密密钥k^{-1}是保密的、新鲜的(不是一个旧的重放密钥),是攻击者I不知道的.保密性规则A3(c),A3(d)表明:如果攻击者I有解密密钥k^{-1}或者m以明文方式传送,那么m不是保密的.

A4(活现性规则).

(a) $-\{...N...\}_{k_{ij}}\wedge B_{p_i,t}(\langle 1 1 k_{ij} p_i p_j\rangle)\wedge B_{p_i,t}(\langle ...1N...\rangle)\rightarrow B_{p_i,t}(\langle 1 p_j\rangle)$

(b) $-\{...N...\}_{k_j^{-1}}\wedge B_{p_i,t}(\langle 0 1 k_j p\rangle)\wedge B_{p_i,t}(\langle 1 1 k_j^{-1} p_j >)\wedge B_{p_i,t}(\langle ...1N...\rangle)\rightarrow B_{p_i,t}(\langle 1 p_j\rangle)$

活现性规则A4(a),A4(b)表明,主体p_i相信意定的通信与方p_j参与了本次会话.

规则A4(a)表示:主体p_i收到了包含信任的新鲜性标识符N的术语$-\{...N...\}_{k_{ij}}$,又由于p_i相信k_{ij}是p_i与p_j的长期共享密钥,所以主体p_i断定只能是意定的通信方p_j加密了自己刚发送的新鲜性标识符N,从而相信p_j真实参与了本次会话.

规则A4(b)表示:主体p_i收到了包含信任的新鲜性标识符N的术语$-\{...N...\}_{k_j^{-1}}$,又由于k_j^{-1}是主体p_j的私钥,所以p_i断定只能是意定的通信方p_j加密了自己刚发送的新鲜性标识符N,从而相信p_j真实参与了本次会话.

A5(关联性规则).

(a) $\pm\{...N...\}_{k_{ij}}\wedge B_{p_i,t}(\langle 1 1 k_{ij} p_i p_j >)\wedge B_{p_i,t}(\langle ...1N...\rangle)\rightarrow B_{p_i,t}(\langle ...1N p_i p_j\rangle)$

(b) $\pm\{...N,p_j...\}_{k_{is}}\wedge B_{p_i,t}(\langle 1 1 k_{is} p_i s\rangle)\wedge B_{p_i,t}(\langle ...1N...\rangle)\rightarrow B_{p_i,t}(\langle ...1N p_i p_j\rangle)$

(c) $-\{...N...\}_{k_j^{-1}}\wedge B_{p_i,t}(\langle 0 1 k_j p\rangle)\wedge B_{p_i,t}(\langle 1 1 k_j^{-1} p_j\rangle)\wedge B_{p_i,t}(\langle ...1N...\rangle)\rightarrow B_{p_i,t}(\langle ...1N p_j\rangle)$

(d) $-\{...N,p_i...\}_{k_j^{-1}}\wedge B_{p_i,t}(\langle 0 1 k_j p\rangle)\wedge B_{p_i,t}(\langle 1 1 k_j^{-1} p_j >)\wedge B_{p_i,t}(\langle ...1N...\rangle)\rightarrow B_{p_i,t}(\langle ...1N p_i p_j\rangle)$

(e) $-\{...N...\}_{k_i}\wedge B_{p_i,t}(\langle 0 1 k_i p\rangle)\wedge B_{p_i,t}(\langle 1 1 k_i^{-1} p_i\rangle)\wedge B_{p_i,t}(\langle ...1N...\rangle)\rightarrow B_{p_i,t}(\langle ...1N p_i\rangle)$

(f) $+\{...p_i,N...\}_{k_j}\wedge B_{p_i,t}(\langle 0 1 k_j p\rangle)\wedge B_{p_i,t}(\langle 1 1 k_j^{-1} p_j\rangle)\wedge B_{p_i,t}(\langle ...1N...\rangle)\rightarrow B_{p_i,t}(\langle ...1N p_i\rangle)$

关联性规则A5(a)~A5(f)表明:主体p_i相信新鲜性标识符N是新鲜的(不是旧的会话密钥),是与通信参与方p_i或(和)p_j相关联的,从而最终确认与协议的某次运行相关.

规则A5(a)表示:主体p_i发送或接收了包含信任的新鲜性标识符N的术语$\pm\{...N...\}_{k_{ij}}$,又由于p_i相信k_{ij}是p_i与p_j的长期共享密钥,所以p_i断定新鲜性标识符N是与p_i和p_j的会话关联的.

规则A5(b)表示:主体p_i发送或接收了包含信任的新鲜性标识符N的术语$\pm\{...N,p_j...\}_{k_{is}}$,又由于$p_i$相信$k_{is}$是$p_i$与可信第三方$S$的长期共享密钥,且在术语中明确指明了$N$和$p_j$的通信有关,故$p_i$相信新鲜性标识符$N$是与$p_i$和$p_j$的会话关联的.

规则A5(c)表示:主体p_i收到了包含信任的新鲜性标识符N的术语$-\{...N...\}_{k_j^{-1}}$,又由于k_j^{-1}是主体p_j的私钥,所以主体p_i断定只能是意定的通信方p_j加密了自己刚发送的新鲜性标识符N,从而N是与p_j的某个特定会话有关的,从而相信N是与p_j关联的.

规则A5(d)表示:主体p_i收到了包含信任的新鲜性标识符N的术语$-\{...N,p_i...\}_{k_j^{-1}}$,又由于$k_j^{-1}$是主体$p_j$的私钥,所以主体$p_i$断定只能是意定的通信方$p_j$加密了自己刚发送的新鲜性标识符$N$,从而$N$是与$p_j$的某个特定会话有关的,由于$p_j$在术语中明确指明了是与$p_i$的通信,从而相信$N$是与$p_i$和$p_j$的某个会话关联的.

规则A5(e)表示:主体p_i收到了包含信任的新鲜性标识符N的术语$-\{...N...\}_{k_i}$,只有p_i拥有该术语的解密密钥——p_i的私钥,所以p_i断定N是与p_i的某个特定会话有关的,从而相信N是与p_i关联的.

规则A5(f)表示:主体p_i发送了包含信任的新鲜性标识符N的术语$+\{...p_i,N...\}_{k_j}$,又由于p_i相信只有主体p_j拥有该术语的解密密钥——p_j的私钥,且在术语中明确指明了N是与p_i的某个特定会话有关的,从而相信N是与p_i关联的.

A6(期望推导规则).

(a) $B_{p_i,t}(\prec\{N,p_j\})\wedge-\{...N...\}_k\wedge B_{p_i,t}(key(p_i,k^{-1}))\wedge B_{p_i,t}(\langle...1N...\rangle)\rightarrow B_{p_i,t}(\langle 1p_j\rangle)$

(b) $B_{p_i,t}(\prec\{N,p_i,p_j\})\wedge-\{...N...\}_k\wedge B_{p_i,t}(key(p_i,k^{-1}))\wedge B_{p_i,t}(\langle...1N...\rangle)\rightarrow B_{p_i,t}(\langle 1p_j\rangle)$

(c) $B_{p_i,t}(\prec\{N,p_i,p_j\})\wedge-\{...N...\}_k\wedge B_{p_i,t}(key(p_i,k^{-1}))\wedge B_{p_i,t}(\langle...1N...\rangle)\rightarrow B_{p_i,t}(\langle...1Np_j\rangle)$

期望推导规则A6(a),A6(b)表明:参与主体p_i拥有期望$B_{p_i,t}(\prec\{N,p_j\})$或者$B_{p_i,t}(\prec\{N,p_i,p_j\})$,即断定只有意定的通信参与方$p_j$才能得到信任的新鲜性标识符$N$.当$p_i$收到了包含$N$的术语$-\{...N...\}_k$时,$p_i$断定只能是$p_j$加密了自己刚发送的新鲜性标识符$N$,从而相信$p_j$参与了本次会话.

A6(c)表明:主体p_i拥有期望$B_{p_i,t}(\prec\{N,p_i,p_j\})$,即断定只有意定的通信参与方$p_j$才能得到信任的新鲜性标识符$N$,并相信$N$是与$p_i$的会话有关的.当$p_i$收到了包含$N$的术语$-\{...N...\}_k$时,$p_i$断定这是$p_j$对$p_i$的挑战$N$的响应,从而相信$N$是与$p_j$关联的.

A7(片段推导规则). $B_{p_i,t}(\Rightarrow\{...N,N'...\}_k)\wedge B_{p_i,t}(\langle...1Np_ip_j\rangle)\rightarrow B_{p_i,t}(\langle...1N'p_ip_j\rangle)$.

片段推导规则A7 表明:如果主体p_i相信新鲜性标识符N'与信任的新鲜性标识符N绑定在相同的会话中,而信任的新鲜性标识符N在本次会话中是新鲜的,是与通信参与者p_i,p_j关联的,那么新鲜性标识符N'也一定是新鲜的、为该次会话生成的.

3 密码协议的安全性分析

3.1 保证认证协议足够安全的安全性条件

定理 1. 假定存在Dolev-Yao模型下的攻击者I,p_i和p_j是密码协议π中的通信主体.p_i相信密码协议π是UA-安全的,其充分必要条件是p_i有信任$B_{p_i,t_S}(\langle 1p_j\rangle)$.

证明:充分性.主体p_i要认证意定通信另一方p_j的身份,这种尝试可能是由p_i发起的,也可能是对意定的通信者p_j发送的某个消息的应答.在本文中,我们把这个尝试看作是对攻击者的一个提问的应答.因为p_i有信任$B_{p_i,t_S}(\langle 1p_j\rangle)$,按照活现性规则A4(a),A4(b),$p_i$一定为该次会话生成了一个询问的新鲜性标识符$N_{p_i}$,那么在对称密钥机制中,$p_i$一定收到了使用$p_i$与$p_j$共享的、大小为$\kappa$的长期加密密钥$k_{ij}$计算的包含$N_{p_i}$的术语;在非对称密钥机制中,$p_i$一定收到了使用大小为$\kappa$的$p_i$私钥计算的包含$N_{p_i}$的术语.即使密码协议中使用的底层密码算法是IND-CPA(indistinguishable chosen plaintext attack)[5]安全的,由我们的新鲜性验证机理,每次协议运行的任意一

条加密消息一定包含一个信任的、新鲜的随机数 N_{p_i} 或 N_{p_j},从而使加密算法成为概率加密算法,由目标密文构造攻击密文也无效.所以,攻击者进行关于 k 的多项式次的 IND-CCA2(adaptive indistinguishable chosen ciphertext attack)[5]攻击训练后,仍然不会找到明密文间的有效联系.于是,当p_i看到对话 $conv_A=(\tau_0,...,N_{p_i})$, $(\tau_2,\{N_{p_i}\}_{k_{ij}},...)$ 或者 $conv_{p_i}=(\tau_0,...,N_{p_i}),(\tau_2,\{N_{p_i}\}_{k_j^{-1}},...)$ 时,它就看到均匀随机串 $\{N_{p_i}\}_{k_{ij}}$ 或者 $\{N_{p_i}\}_{k_j^{-1}}$ 是用它自己生成的 N_{p_i} 计算的,所以它可以确信这个术语不是它意定的通信另一方p_j计算(换句话说,是攻击者计算的)的比特串的概率约为 $2^{-\kappa}$.因此p_i可以相信,它的意定通信参与者p_j有一个对话以 $conv_{p_j}=(\tau_1,N_{p_i},\{N_{p_i}\}_{k_{ij}})$ 或者 $conv_{p_j}=(\tau_1,N_{p_i},\{N_{p_i}\}_{k_j^{-1}})$ 为前缀.这必然向p_i证明了与 $conv_{p_i}$ 匹配的对话 $conv_{p_j}$ 的存在性,而且这个对话已经以(关于κ的)压倒性概率 $1-2^{-\kappa}$被它意定通信者p_j计算过了.

所以,如果p_i有信任 $B_{p_i,t_\$}(\langle 1p_j\rangle)$,那么攻击者成功的概率只是一个可忽略量,根据定义 3,p_i可以相信认证密码协议π是 UA-安全的.

必要性.如果密码协议π是UA-安全的,那么p_i一定有信任 $B_{p_i,t_\$}(\langle 1p_j\rangle)$.如果$p_i$没有信任 $B_{p_i,t_\$}(\langle 1p_j\rangle)$,那么按照活现性规则A4(a),A4(b),意味着p_i将旧的询问发送给p_j(所以攻击者I可以伪装成p_j回放一个旧的消息响应给p_i),或者p_j不需要对p_i为该次会话生成的询问响应,于是I就可以伪装成主体p_j,从而密码协议π是UA-安全的是不可能的.至此,我们可以相信UA-安全的量化指标是充分必要的. □

定理 2. 假定存在Dolev-Yao模型下的攻击者I,p_i和p_j是密码协议π中的通信主体.密码协议π是MA-安全的,其充分必要条件是p_i有信任 $B_{p_i,t_\$}(\langle 1p_j\rangle)$,$p_j$有信任 $B_{p_j,t_\$}(\langle 1p_i\rangle)$.

证明:充分性.类似于定理 1,p_i和p_j都可以确信它的意定通信对方以压倒性的概率生成了一个与记录的 $conv_{p_i}$ (或者 $conv_{p_j}$)相匹配的对话.具体步骤略.

必要性.类似定理 1,如果密码协议π是双方认证安全的,那么p_i一定有信任 $B_{p_i,t_\$}(\langle 1p_j\rangle)$,$p_j$有信任 $B_{p_j,t_\$}(\langle 1p_i\rangle)$.具体步骤略. □

定理 3. 假定存在Dolev-Yao模型下的攻击者I,p_i和p_j是密码协议π中的通信主体.p_i相信密码协议π是UK-安全的,其充分必要条件是p_i有信任多集$\lfloor\langle 1p_j\rangle,\langle 11kp_ip_j\rangle\rfloor$.

证明:充分性.我们首先证明密码协议π满足安全定义 5(1)的条件.因为p_i有信任 $B_{p_i,t_\$}(\langle 1p_j\rangle)$,按照定理 1,参与者$p_i$可以确信它的意定通信对方$p_j$以压倒性的概率生成了一个与记录的 $conv_{p_i}$ 相匹配的对话 $conv_{p_j}$,即p_i相信声明为通信方p_j的主体一定对同一会话进行了响应.因为p_i有信任 $B_{p_i,t_\$}(\langle 1kp_ip_j\rangle)$, 按照关联性规则A5,密钥$k$的关联性决定了本次协议运行的主体是$p_i$,$p_j$,$k$的新鲜性决定了$k$是为$p_i$,$p_j$间的该次协议运行产生的,从而决定了$k$与其他会话中生成的会话密钥是不同的.也就是说,未被攻破的、声明为通信方p_j的主体一定为该次会话输出了与p_i相同的会话密钥k.

下面证明密码协议π满足定义 5(2)的条件.回想一下,攻击者I是一个概率多项式时间机器,对通信链路具有完全的控制能力,能进行密码课程训练.l是允许攻击者申请的会话次数的上限.k是密码协议的某次运行产生的一个新的会话密钥.让p_i和攻击者进行定义 5 中的游戏.假设bad是k的信息在适应性选择密文训练中可能被泄漏的事件.I_{wins}是攻击者I正确猜测比特b的概率.显然,在事件bad没有发生的情况下,由于k是由p_j随机选取的概率分布的一个新会话密钥值,所以询问比特b独立于询问密文比特b',这样我们就有

$$Prob[I_{wins}\mid\overline{Bad}]=\frac{1}{2},$$

又因为

$$Prob[I_{wins}\mid\overline{Bad}]=\frac{Prob[I_{wins}\cap\overline{Bad}]}{Prob[\overline{Bad}]},$$

则有

$$\frac{Prob[I_{wins}\cap\overline{Bad}]}{Prob[\overline{Bad}]}=\frac{1}{2},$$

$$Prob[I_{wins}\cap\overline{Bad}]=\frac{1}{2}Prob[\overline{Bad}]=\frac{1}{2}(1-Prob[Bad]).$$

另一方面, $Prob[I_{wins}]=Prob[I_{wins}\cap Bad]+Prob[I_{wins}\cap \overline{Bad}]$,

所以, $Prob[I_{wins}]\le Prob[Bad]+Prob[I_{wins}\cap \overline{Bad}]=Prob[Bad]+\frac{1}{2}(1-Prob[Bad])=\frac{1}{2}(1+Prob[Bad])$.

在密码协议中,即使使用的底层密码算法是 IND-CPA 安全的,由我们的新鲜性验证机理,每次协议运行的任意一条加密消息一定包含一个信任的、新鲜的随机数 N_{p_i} 或 N_{p_j},从而使加密算法成为概率加密算法,由目标密文构造攻击密文无效,所以攻击者进行关于k的多项式次的IND-CCA2 攻击训练后,仍然不会找到明、密文之间的有效联系.那么,在安全参数κ的前提下,密码算法泄漏新会话密钥k的信息的概率为一个可忽略量Adv;即使攻击者提出了多达l次的会话训练课程,密码算法本身泄漏新会话密钥k的信息($bad1$)的概率也仅为$l\times Adv$;由UK-安全条件(1),参与协议π运行的主体p_i相信p_j真实地参与了协议运行,攻击者I要伪装成主体p_j是不可能的,因此明确的意定通信方p_j主动泄漏新会话密钥k的信息($bad2$)的概率为 0;由UK-安全条件(2),与攻击者玩攻击游戏的主体p_i主动泄漏新会话密钥k的信息($bad3$)的概率为 0.因为p_i有信任多集$\lfloor\langle 11kp_ip_j\rangle\rfloor$,即$k$是新鲜的,又是与此次运行的通信参与者$p_i$,$p_j$关联的,从而决定了$k$是密码协议的某次运行产生的一个新的会话密钥,且是与其他会话密钥不同的.因此,攻击者I用自己与某一个诚实通信方建立的会话密钥来迷惑通信方p_i,使它相信是p_i,p_j之间的新会话密钥($bad4$)的概率为 0.所以,

$$Prob[Bad]=Prob[Bad1]+Prob[Bad2]+Prob[Bad3]+Prob[Bad4]=Adv\times\ell.$$

从而有 $$Prob[I_{wins}]\le\frac{1}{2}(1+Prob[Bad])=\frac{1}{2}(1+Adv\times\ell)=\frac{1}{2}+\frac{Adv\times\ell}{2}.$$

由于攻击者I是一个多项式时间机器,所以在安全参数κ的前提下,攻击者I正确猜测比特b的概率不大于 1/2 加一个可忽略量.根据定义 5,p_i可以相信认证密码协议π是UK-安全的.

必要性.如果密码协议π是UK-安全的,那么p_i一定有信任多集$\lfloor\langle 1p_j\rangle,\langle 11kp_ip_j\rangle\rfloor$.如果$p_i$没有信任$B_{p_i,t_S}(\langle 1p_j\rangle)$,那么按照活现性规则A4,意味着$p_i$使用了旧的询问发送给$p_j$(也就是说,攻击者$I$可以伪装成$p_j$回放一个旧的消息响应给$p_i$),或者$p_j$不需要对$p_i$为该次会话生成的询问 N_{p_i} 响应,于是攻击者I就可以伪装成主体p_j,从而发起针对密码协议π的攻击.典型的例子见Otway-Rees protocol协议[15]、Woo-Lam-Abadi协议[2].

如果p_i相信会话密钥k是不保密发送的,即信任$B_{p_i,t_S}(\langle 01kp_ip_j\rangle)$,那么攻击者$I$在进行定义 5 中的攻击游戏时,正确猜测比特$b$的概率为 1,密码协议$\pi$就不可能是UK-安全的.如果$p_i$相信会话密钥$k$是保密发送的,但对于会话密钥$k$是否新鲜即是否是为该次运行新生成的不能确定,即有$B_{p_i,t_S}(\langle 1...kp_ip_j\rangle)$,于是攻击者$I$可以选择一个已经泄漏的会话密钥值$k'$,并将记录的含有该会话值$k'$的消息回放给$p_i$作为响应.典型的例子见Needham-Schroeder共享密钥认证协议[3,16].如果p_i相信会话密钥k是保密发送的,且是新鲜的,但没有与协议运行的主体关联,即有$B_{p_i,t_S}(\langle 11k...\rangle)$,那么攻击者$I$可以用自己与某一诚实的通信方建立的会话密钥来迷惑另一诚实的通信方,使他们相信是两诚实的通信方之间的新会话密钥,典型的例子见Needham-Schroeder公钥认证协议[9]、传感器网络环境下基于Kerberos的对密钥管理方案[17].

至此,我们可以相信 UK-安全的量化指标是充分必要的. □

定理 4. 假定存在Dolev-Yao模型下的攻击者I,p_i和p_j是密码协议π中的通信主体.密码协议π是MK-安全的,其充分必要条件是p_i有信任多集$\lfloor\langle 1p_j\rangle,\langle 11kp_ip_j\rangle\rfloor$,$p_j$有信任多集$\lfloor\langle 1p_i\rangle,\langle 11kp_ip_j\rangle\rfloor$.

证明:类似于定理 3.具体步骤略. □

3.2 安全性条件验证

假设p_i与p_j为协议参与主体,S为可信第三方,k为生成的新会话密钥,信任多集方法的分析步骤如下:

(1) 给出协议初始信任集合.

非对称密码体制:每个通信参与者在协议运行前已经知道了自己的私钥和其他参与者的公钥.协议的初始集合为 $B_{p_i,t_0}(\langle 11k_i^{-1}p_i\rangle,\langle 11k_j^{-1}p_j\rangle,\langle 01k_ip\rangle,\langle 01k_jp\rangle)$ 和 $B_{p_j,t_0}(\langle 11k_j^{-1}p_j\rangle,\langle 11k_i^{-1}p_i\rangle,\langle 01k_ip\rangle,\langle 01k_jp\rangle)$.

对称密码体制:每个通信参与者在协议运行前已经知道了自己与通信对方(或者与可信第三方)的长期共享

密钥.协议的初始集合为 $B_{p_i,t_0}(\langle 11k_{ij}p_ip_j\rangle)$ 和 $B_{p_j,t_0}(\langle 11k_{ij}p_ip_j\rangle)$ (或者 $B_{p_i,t_0}(\langle 11k_{is}p_is\rangle)$ 和 $B_{p_j,t_0}(\langle 11k_{js}p_js\rangle)$).

(2) 形式化说明密码协议将要达成的目标,即安全条件:

I. 单方认证安全:主体p_i(或p_j)要确认p_j(或p_i)的身份.协议的安全目标为 $b_{p_i,t_\$}=\lfloor\langle 1p_j\rangle\rfloor$(或 $b_{p_j,t_\$}=\lfloor\langle 1p_i\rangle\rfloor$).

II. 双方认证安全:主体p_i和p_j要互相确认身份.协议的安全目标为 $b_{p_i,t_\$}=\lfloor\langle 1p_j\rangle\rfloor$和 $b_{p_j,t_\$}=\lfloor\langle 1p_i\rangle\rfloor$.

III. 单方密钥安全:主体p_i(或p_j)要认证p_j(或p_i)的身份,并相信p_j(或p_i)生成的密钥k能够为敏感数据提供一个安全的通信信道.协议的安全目标为 $b_{p_i,t_\$}=\lfloor\langle 11kp_ip_j\rangle\langle 1p_j\rangle\rfloor$(或 $b_{p_j,t_\$}=\lfloor\langle 11kp_ip_j\rangle\langle 1p_i\rangle\rfloor$).

IV. 双方密钥安全:对密钥传输机制,主体p_i和p_j要互相认证身份,协议输出的共享密钥k来自参与协议的某一个主体或者可信第三方.协议的安全目标为 $b_{p_i,t_\$}=\lfloor\langle 11kp_ip_j\rangle\langle 1p_j\rangle\rfloor$和 $b_{p_j,t_\$}=\lfloor\langle 11kp_ip_j\rangle\langle 1p_i\rangle\rfloor$.

对密钥协商机制,主体p_i和p_j要互相认证身份,协议输出的共享密钥k由p_i和p_j的随机输入 N_{p_i} 和 N_{p_j} 共同生成.协议的安全目标为 $b_{p_i,t_\$}=\lfloor\langle 11N_{p_i}p_ip_j\rangle,\langle 11N_{p_j}p_ip_j\rangle\langle 1p_j\rangle\rfloor$ 和 $b_{p_j,t_\$}=\lfloor\langle 11N_{p_i}p_ip_j\rangle,\langle 11N_{p_j}p_ip_j\rangle\langle 1p_i\rangle\rfloor$.

(3) 在发送或者接收每一句消息(Message*)后,对要分析的密码协议分别提取包含信任的新鲜性标识符的消息,即符号术语.基于每个通信参与主体已有的信任和提取的带符号术语,运用推导规则和公理,建立每个通信参与主体关于密码协议安全性的信任,即安全属性的集合,直至协议运行结束.

(4) 将实际得到的安全属性的集合与步骤(1)中的安全目标比较.如果期望的安全目标没有满足,就意味着该协议存在安全属性的缺失,可以直接构造针对该协议的攻击:

I. 主体活现性缺失:伪装成该主体发起针对该认证协议的攻击.

II. 新会话密钥的保密性缺失:攻击者掌握了新会话密钥.

III. 新会话密钥的新鲜性缺失:重放攻击,使用一个旧的会话密钥欺骗某个诚实的协议参与者.

IV. 新会话密钥的关联性缺失:使用与其他协议运行实例中的主体相关联的会话密钥来欺骗某个诚实的协议参与者.如果拥有主体活现性信任,而新会话密钥的关联性缺失,则暗示了一个交错攻击.

4 信任多集方法的应用

4.1 应用实例

4.1.1 原始的 Needham-Schroeder 公钥认证密码协议分析

Needham-Schroeder公钥认证密码协议[3](简称N-S协议)是一个密钥协商协议,新会话密钥由协议参与者A和B给出的随机输入N_a,N_b共同生成(MK-安全).本文采用Dolev-Yao模型[14]中的密码协议形式化符号表示.

N-S 协议初始集合:

$$b_{A,t_0}=\lfloor\langle 11k_a^{-1}A\rangle,\langle 11k_b^{-1}B\rangle,\langle 01k_bp\rangle,\langle 01k_ap\rangle\rfloor,\ b_{B,t_0}=\lfloor\langle 11k_b^{-1}B\rangle,\langle 11k_a^{-1}A\rangle,\langle 01k_ap\rangle,\langle 01k_bp\rangle\rfloor.$$

N-S 协议安全目标:

$$b_{A,t_\$}=\lfloor\langle 11N_aAB\rangle,\langle 11N_bAB\rangle,\langle 1B\rangle\rfloor,\ b_{B,t_\$}=\lfloor\langle 11N_aAB\rangle,\langle 11N_bAB\rangle,\langle 1A\rangle\rfloor.$$

发送 Message 1 后,应用公理 A0,A3(b),A5(f),A 有 $B_{A,t_1}(\langle 11N_aA\rangle)$; 应用公理 A2(c),$A$ 有 $B_{A,t_1}(\prec\{N_a,A,B\})$.

收到 Message 1 后,应用公理 A3(a),B 有 $B_{B,t_1}(\langle 1...N_a...\rangle)$.

发送 Message 2 后,应用公理 A0,A3(b),B 有 $B_{B,t_2}(\langle 11N_b...\rangle)$; 应用公理 A2(b),$B$ 有 $B_{B,t_2}(\prec\{N_b,A\})$.

收到Message 2 后,应用公理A1(c),A有 $B_{A,t_2}(\Rightarrow\{...N_a,N_b...\}_{k_a})$; 应用规则R1,R2 和公理A6(b),A6(c),A有 $B_{A,t_2}(\langle 1B\rangle)$, $B_{A,t_2}(\langle ...1N_aB\rangle)$;应用规则R5,A有 $B_{A,t_2}(\langle 11N_aBA\rangle)$;应用公理A7,A有 $B_{A,t_2}(\langle 11N_bBA\rangle)$.应用规则R3,R4,R5,A有 $b_{A,t_2}=\lfloor\langle 11N_aAB\rangle,\langle 11N_bAB\rangle,\langle 1B\rangle\rfloor$.

收到Message 3 后,应用规则R2,R1 和公理A6(a),B有 $B_{B,t_3}(\langle 1A\rangle)$;应用公理A5(e)和规则R5,B有 $B_{A,t_3}(\langle 11N_bB\rangle)$.应用规则R3,R4,R5,B仅有 $b_{B,t_3}=\lfloor\langle 1\ldots N_a\ldots\rangle,\langle 11N_bB\rangle,\langle 1A\rangle\rfloor$.

我们的分析结果表明,从参与者B的角度出发,N-S协议中的新鲜性标识符N_a存在新鲜性和关联性安全属性

的缺失,明确指出的安全属性缺失帮助我们构造而不仅仅是发现针对N-S协议的攻击:在协议运行结束后,主体B虽然能够断定主体A真实地参加了通信,但不能断定N_a是与主体A和B关联的,即 $B_{B,t_\$}(\langle 1...N_a...\rangle)$, 从而攻击者可以使用它与其他诚实参与者的随机数 N'_a 来迷惑主体B.在此处,主体B能够断定主体A的确参与了通信 $B_{B,t_\$}(\langle 1A\rangle)$, 表明主体$A$在攻击者的攻击中必然要起到一个加解密预言机的作用,从而决定了针对N-S协议的攻击必然需要协议的两个运行实例,是一个交错攻击.我们很高兴地看到,这个构造而不仅仅是发现的攻击与Lowe使用FDR工具发现的漏洞本质上是相同的[1].

4.1.2 改进的 Needham-Schroeder 公钥密码协议分析

在文献[9]中,Lowe 对原始的 N-S 协议 Message 2 进行了改进: $\{B,N_a,N_b\}_{k_a}$, 简称为 N-S-L 协议.Lowe 使用 FDR 工具证明了 N-S-L 协议的正确性.我们给出基于信任多集形式化方法的 N-S-L 协议安全性分析.

与原始的 N-S 协议相同的证明部分不再重复.

发送Message 2 后,应用公理A2(c),A5(f),B有 $B_{B,t_2}(\prec\{N_b,B,A\})$, $B_{B,t_2}(\langle ...1N_bB\rangle)$;应用公理A1(g),$B$有 $B_{B,t_2}(\Rightarrow\{...N_a,N_b...\}_{k_a})$.收到Message 3 后,应用公理A6(c),A7,R5,B有 $B_{B,t_3}(\langle 11N_aBA\rangle)$.因此,$B$有 $b_{B,t_\$}=\llcorner\langle 11N_aAB\rangle,\langle 11N_bAB\rangle,\langle 1A\rangle\lrcorner$.至此,$A$和$B$都相信N-S-L协议是MK-安全的.

4.1.3 传感器网络环境下一个基于 Kerberos 的对密钥管理方案

传感器网络环境下,基于Kerberos的对密钥管理方案[17]在密钥颁发中心(Key Distribution Center,简称KDC)的帮助下在两个节点A和B之间建立临时会话密钥k_{ab}.ID_A,ID_B,ID_I是节点A、B和攻击者I的标识符,KDC_j是第j个KDC的标识符.每个传感器节点A,B与KDC(KDC_j)之间都预先共享一个密钥K_{aj},K_{bj}.N_a是随机数,$ticket_B=(k_{ab},A,L)_{K_{bj}}$,$T_a$是时间标记,$L$是密钥生命期.该协议与密钥建立有关的部分如下:

Message 1. $A\rightarrow KDC_j$: KDC_j,ID_A,ID_B,N_a

Message 2. $KDC_j\rightarrow A$: $ID_A,KDC_j,ticket_B,N_a,\{k_{ab},ID_B,N_a,L\}_{K_{aj}}$

Message 3. $A\rightarrow B$: $ID_B,ID_A,ticket_B,\{ID_B,T_a\}_{k_{ab}}$

Message 4. $B\rightarrow A$: $ID_A,ID_B,\{T_a\}_{k_{ab}}$

传感器网络的对密钥管理方案初始集合: $b_{A,t_0}=\llcorner\langle 11K_{aj}A\ KDC_j\rangle\lrcorner$和 $b_{B,t_0}=\llcorner\langle 11K_{bj}B\ KDC_j\rangle\lrcorner$.

传感器网络的对密钥管理方案安全目标: $b_{A,t_\$}=\llcorner\langle 1B\rangle,\langle 11k_{ab}AB\rangle\lrcorner$及 $b_{B,t_\$}=\llcorner\langle 1A\rangle,\langle 11k_{ab}AB\rangle\lrcorner$.

发送 Message 1 后,应用公理 A0,A 有 $B_{B,t_1}(\langle 01N_a...\rangle)$.

发送 Message 2 后,应用公理 A1(b),A5(b),A3(a),A7,A 有 $B_{A,t_2}(\Rightarrow\{...k_{ab},N_a...\}_{K_{aj}})$, $B_{A,t_2}(\langle 01N_aBA\rangle)$, $B_{A,t_2}(\langle 1...k_{ab}...\rangle)$, $B_{A,t_2}(\langle ...1k_{ab}BA\rangle)$.

发送 Message 3 后,应用公理 A0,A2(a),A 有 $B_{A,t_3}(\langle ...1T_a...\rangle)$, $B_{A,t_3}(\prec\{T_a,A,B\})$. 收到 Message 3 后,应用公理 A3(a),B 有 $B_{B,t_3}(\langle 1...k_{ab}...\rangle)$.

收到 Message 4 后,应用公理 A4(a),A 有 $B_{A,t_4}(\langle 1B\rangle)$.

至此,A有 $b_{A,t_\$}=\llcorner\langle 1B\rangle,\langle 11k_{ab}AB\rangle\lrcorner$,$B$有 $b_{B,t_\$}=\llcorner\langle\ldots A\rangle,\langle 1\ldots k_{ab}\ldots\rangle\lrcorner$.$B$建立的密码协议安全属性存在缺失,由$k_{ab}$新鲜性的缺失,类似于Needham-Schroeder共享密钥认证协议[16],使用泄漏的旧密钥 k'_{ab} 构造攻击:

Message 3. $I(A)\rightarrow B$: $ID_B,ID_A,ticket_B,\{ID_B,T_I\}_{k'_{ab}}$

Message 4. $B\rightarrow I(A)$: $ID_A,ID_B,\{T_I\}_{k'_{ab}}$

4.1.4 改进的传感器网络环境下对密钥管理方案的分析

为修补重放旧$ticket_B$进行攻击的漏洞,研究人员提出了一个$ticket_B$的变种($ticket_B=(k_{ab},N_a,L)_{K_{bj}}$)来修补这个漏洞[17].然而,节点$B$并不知道$N_a$是新鲜的,因此,在收到Message 3 后,$B$还是得不到任何新的信任.也就是说,在协议运行结束时,B仍然不能认证A的主体活现性,不能认证临时会话密钥k_{ab}的新鲜性,以及k_{ab}与节点A和B的关联性.由于新$ticket_B$不含A的身份信息,从而使修改后的协议更容易受到攻击.我们的攻击如下:

Message 1. $I\rightarrow KDC_j$: KDC_j,ID_I,ID_B,N_I

Message 2. $KDC_j \rightarrow I$: $ID_I, KDC_j, ticket_B, N_I, (k_{ab}, ID_B, N_I, L)_{K_{Ij}}$

Message 3. $I(A) \rightarrow B$: $ID_B, ID_A, ticket_B, (ID_B, T_I)_{k_{ab}}$

Message 4. $B \rightarrow I(A)$: $ID_A, ID_B, (T_I)_{K_{ab}}$

这是一个完善的攻击过程.节点B认为它与节点A建立了一个会话密钥k_{ab},而实际上却是与攻击者I共 享k_{ab}.

4.2 分析与比较

实例分析表明,信任多集方法提出了严格而又精确的保证密码协议足够安全的量化指标,以及通信参与者建立关于密码协议安全性的信任的方法.与已有的密码协议分析方法进行对比,信任多集方法有如下一些特点:

(1) 信任多集方法明确指出了保证密码协议足够安全的量化指标,这些量化指标不仅是充分的,而且是必要的.利用信任多集方法对密码协议进行分析,分析结果对协议是否安全给出了明确结论:要么证明了一个密码协议是安全的,要么指出了不安全协议的不足.所以,信任多集方法不仅是证明密码协议正确性的方法,而且是查找协议错误的方法.

信任多集方法只处理包含了信任的新鲜性标识符的消息,并从中推导出参与主体关于密码协议安全性的信任,即密码协议的安全属性.BAN逻辑的推理规则如消息含义规则没有有效区分消息是否新鲜的内容,造成其他主体可以发送这些消息的备份,导致 BAN 逻辑证明正确的协议仍可能存在漏洞.因此,信任多集方法与同样基于逻辑推理的 BAN 逻辑的逻辑推理基础是不同的,没有包含信任的新鲜性标识符的消息在信任多集方法中不会被提取为术语.基于定理证明的方法包括 Strand Space 等是证明密码协议正确性的方法,但它们的分析过程与攻击者能力的具体形式化相关.基于模型检验的分析方法是有效查找密码协议错误的方法.

(2) 基于信任多集方法的安全性分析所指出的密码协议安全属性缺失,可以帮助研究人员直接构造攻击,而不仅仅是发现某种攻击.以双向认证的密钥交换协议为例,如果参与通信的主体身份没有得到认证,则可以构造平行攻击、反射攻击[5];如果通信某一方的身份得到了认证,而密钥没有与本次协议运行的主体关联起来,则可以构造交错攻击[1];如果密钥不能保证是为本次运行产生的,则可以构造密钥复用的攻击[16].

(3) 基于信任多集方法的安全性分析独立于密码协议和攻击者行为的具体形式化,与并发的多协议运行环境具体形式化描述无关.在信任多集方法中,每个通信参与者只处理该主体相信新鲜的消息即术语,不需要对密码协议进行具体形式化.信任多集方法安全属性的建立仅取决于已有的信任和新鲜性消息,与通信环境的具体形式化描述无关,从而无须给出攻击者行为的具体形式化.但在基于模型检验的分析方法和 Strand Space 方法中,安全性的建立与攻击者行为以及密码协议的具体形式化描述相关.但是,新漏洞常常是由一种新的攻击行为的提出而找到的.

(4) 信任多集方法具有独立的、明确的语义,消除了由于形式化公式的含义和推理规则的推理能力所引起的理解模糊问题.所以,信任多集方法不仅可以用于手工分析,而且便于在计算机中实现、开发出自动验证系统.

表 1 是信任多集形式化方法与已有的一些形式化分析方法的特点比较,√表示该形式化方法具有该特点.

Table 1 Comparison with previous formalisms

表 1 与已有形式化分析方法的比较

Formalisms	Prove correctness	Find faults	Construct attacks	Independent of protocol formal specification	Independent of the concrete formalization of attacks' possible behaviors	Independent of concurrent protocol run	Automation
BAN-Like logic	√			√	√		√
Computational model	√			√	√	√	
Model checking		√					√
Theorem proving	√						
Strand space	√						√
Authentication test	√						√
CK model	√						
Belief multisets	√	√	√	√	√	√	√

4.3 局限性与自动化验证

信任多集形式化方法的核心思想和保证认证协议足够安全的充分必要条件是明确的,密码协议初始状态的形式化描述和安全属性逻辑推理的过程是严格的,但是信任多集形式化方法中公理的完备性仍然不够,根据不同的应用,需要对给出的信任多集形式化方法中的公理做进一步扩充.

基于信任多集方法分析密码协议具有严格的形式化描述和推理过程,这蕴涵了自动化验证实现的可能.无论是对基于对称密码体制的密码协议,还是基于非对称密码体制的密码协议,协议的初始状态和安全目标都可以在信任多集形式化方法中明确表示(第 3.2 节).应用信任多集中带符号的术语、推导规则以及公理(第 2.2 节、第 2.3 节),从协议的初始状态即信任多集的初始集合开始推证,得到实际建立的关于密码协议安全性的安全属性的集合,并比较是否满足期望的安全目标.与期望的安全目标的比较结果,要么证明了密码协议的正确性,要么查找到了密码协议的错误,并指出了构造攻击的结构.所以说,信任多集形式化方法简洁而又严谨地指出了实际建立的密码协议安全属性,不仅可用于手工的分析,而且便于在计算机中实现、开发出自动验证系统.

我们正在开发信任多集形式化方法自动验证系统,已经实现了密码协议安全属性的部分自动推理功能.但是,已开发的自动验证系统中的规则和公理是固定的,自动验证系统需要进一步扩充,以允许用户输入新的规则来满足不同的安全需求.另外,新鲜性术语的提取目前仍由人工完成,需要从基于 Dolev-Yao 模型建立的密码协议表示中由验证系统自动提取,从而使密码协议安全验证进一步自动化.

5 结 论

本文提出了用于密码协议安全性分析和设计的信任多集形式化方法.信任多集形式化方法的核心思想是:对每个通信参与主体而言,密码协议的安全性取决于发送或者接收的、包含自身已相信新鲜的新鲜性标识符的单向变换.首先,基于匹配对话的认证性和基于不可区分性的保密性,给出了单方认证安全、双方认证安全、单方密钥安全和双方密钥安全 4 种安全性定义.随后,引入了信任多集形式化分析方法,明确了保证密码协议 4 种安全性的量化安全指标,并给出了这些量化指标在计算模型下满足相关安全定义的证明.以 Needham-Schroeder 公钥认证协议、传感器网络环境下一个基于 Kerberos 的对密钥管理方案为例,说明了如何应用信任多集方法分析密码协议的安全属性.信任多集形式化方法准确地分析了密码协议取得的安全性,分析的结果或者表明该密码协议已经达到了预期的安全目标,或者指出了被分析的不安全协议的不足,明确指出的安全属性的缺失给出了直接构造攻击的方法.信任多集形式化方法不仅给出了保证密码协议足够安全的精确量化指标,而且提供了清晰的语义和统一的密码协议分析模型,在我们的研究工作中非常有用.对我们来说,分析密码协议已经变得非常有趣而令人激动.表 2 列出了部分密码协议的安全性分析结果.

本文主要研究了密码协议的保密性和认证性.根据信任多集的核心思想,在未来的工作中,我们将对更多的安全属性,如不可否认性和公平性等进行分析.我们希望也相信,信任多集形式化方法能够帮助更多的研究者改善他们的密码通信协议.

Table 2 Analysis of some cryptographic protocols based on belief multisets

表 2 基于信任多集的部分密码协议安全性分析结果

Protocols	Protocol analysis results	Remarks
N-S public key[3]	$\begin{cases} b_{A,t_5} = \lfloor \langle 1B\rangle, \langle 11N_aAB\rangle, \langle 11N_bAB\rangle \rfloor \\ b_{B,t_5} = \lfloor \langle 1A\rangle, \langle 1...N_a...\rangle, \langle 11N_bAB\rangle \rfloor \end{cases}$	Interleaving attack by confusing N_a
N-S-L public key[9]	$\begin{cases} b_{A,t_5} = \lfloor \langle 1B\rangle, \langle 11N_aAB\rangle, \langle 11N_bAB\rangle \rfloor \\ b_{B,t_5} = \lfloor \langle 1A\rangle, \langle 11N_aAB\rangle, \langle 11N_bAB\rangle \rfloor \end{cases}$	Secure
Refined N-S public[5]	$\begin{cases} b_{A,t_5} = \lfloor \langle 1B\rangle, \langle 11N_aAB\rangle, \langle 11N_bAB\rangle \rfloor \\ b_{B,t_5} = \lfloor \langle 1A\rangle, \langle 11N_aAB\rangle, \langle 11N_bAB\rangle \rfloor \end{cases}$	Secure
N-S shared key [3,16]	$\begin{cases} b_{A,t_5} = \lfloor \langle 1B\rangle, \langle 11k_{ab}AB\rangle \rfloor \\ b_{B,t_5} = \lfloor \langle ...A\rangle, \langle 1...k_{ab}...\rangle \rfloor \end{cases}$	Attack by replaying a promised k'_{ab}
Otway-Rees protocol[15]	$\begin{cases} b_{A,t_5} = \lfloor \langle ...B\rangle, \langle 11k_{ab}AB\rangle \rfloor \\ b_{B,t_5} = \lfloor \langle ...A\rangle, \langle 11k_{ab}AB\rangle \rfloor \end{cases}$	Attack by impersonating A or B
Woo-Lam-Abadi[2]	$\begin{cases} b_{A,t_5} = \lfloor \langle ...B\rangle, \langle ...S\rangle, \langle 0...N_b...\rangle \rfloor \\ b_{B,t_5} = \lfloor \langle ...A\rangle, \langle 1S\rangle, \langle 01N_bAB\rangle \rfloor \end{cases}$	Attack by impersonating A
Neuman-Stubblebine[18]	$\begin{cases} b_{A,t_5} = \lfloor \langle ...B\rangle, \langle 1S\rangle, \langle 01N_aAB\rangle, \langle 0...N_b...\rangle, \langle 11kAB\rangle \rfloor \\ b_{B,t_5} = \lfloor \langle ...A\rangle, \langle ...S\rangle, \langle 0...N_a...\rangle, \langle 01N_bAB\rangle, \langle 1...kAB...\rangle \rfloor \end{cases}$	Attack by impersonating A or B
Pair-Key based on Kerberos in WLANS[17]	$\begin{cases} b_{A,t_5} = \lfloor \langle 1B\rangle, \langle 11kAB\rangle \rfloor \\ b_{B,t_5} = \lfloor \langle ...A\rangle, \langle 1...k...\rangle \rfloor \end{cases}$	Attack by impersonating A
IEEE 802.11i 4-Way Handshake[19]	$\begin{cases} b_{S,t_5} = \lfloor \langle 1A\rangle, \langle 11PTKAS\rangle \rfloor \\ b_{A,t_5} = \lfloor \langle 1S\rangle, \langle 11PTKAS\rangle \rfloor \end{cases}$	The IEEE 802.11i 4-Way Handshake is secure if PMK (pairwise master key) is secure

References:

[1] Lowe G. An attack on the needham-schroeder public key authentication protocol. Information Processing Letters, 1995,56(3): 131−133.

[2] Abadi M, Needham R. Prudent engineering practice for cryptographic protocols. IEEE Trans. on Software Engineering, 1996,21(1): 6−15.

[3] Needham R, Schroeder MD. Using encryption for authentication in large network of computers. Communications of the ACM, 1978,21(12):993−999.

[4] Burrows M, Needham R. A logic of authentication. ACM Trans. on Computer Systems, 1990,8(1):18−36.

[5] Mao W. Modern Cryptography: Theory and Practice. Beijing: Publishing House of Electronic Industry Press, 2004.

[6] Goldwasser S, Micali S. Probabilistic encryption. Journal of Computer & System Sciences, 1984,28(2):270−299.

[7] Bellare M, Rogaway P. Entity authentication and key distribution. In: Stinson DR, ed. Advances in Cryptology-CRYPTO'93. LNCS 773, New York: Springer-Verlag, 1993. 232−249.

[8] Bellare M, Rogaway P. Random oracles are practical: A paradigm for designing efficient protocols. In: Proc. of the 1st ACM Conf. on Computer and Communications Security. New York: ACM Press, 1993. 62−73.

[9] Lowe G. Breaking and fixing the needham-schroeder public key protocol using FDR. In: Margaria T, Steffen B, eds. Tools and Algorithms for Construction and Analysis of Systems, Second International Workshop, TACAS'96, Vol.1055. Passau: Springer-Verlag, 1996. 147−166.

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

[11] Canetti R, Krawczyk H. Analysis of key-exchange protocols and their use for building secure channels. In: Pfitzmann B, ed. Proc. of the EUROCRYPT 2001. LNCS 2045, Berlin: Springer-Verlag, 2001. 453−474.

[12] Fabrega F, Herzog J, Guttman J. Strand spaces: Why is a security protocol correct? In: Proc. of the 1998 IEEE Symp. on Security and Privacy. Los Alamitos: IEEE Computer Society Press, 1998. 160−171.

[13] Guttman J, Thayer F. Authentication tests. In: Proc. of the 2000 IEEE Symp. on Security and Privacy. Los Alamitos: IEEE Computer Society Press, 2000. 96−109.

[14] Dolev D, Yao AC. On the security of public key protocols. IEEE Trans. on Information Theory, 1983,IT-29(2):198−208.

[15] Otway D, Rees O. Efficient and timely mutual authentication. Operating Systems Review, 1987,21(1):8−10.

[16] Denning D, Sacco G. Timestamps in key distribution protocols. Communications of the ACM, 1978,24(8):533−536.

[17] Carman DW, Kruus PS, Matt BJ. Constraints and approaches for distributed sensor network security. Technical Report, #00-010, NAI Labs., 2000. http://icsd.i2r.a-star.edu.sg/SecureSensor/papers/nailabs_report_00-010_final.pdf

[18] Guttman J, Thayer F. Protocol independence through disjoint encryption. In: Lee S, ed. Proc. of the 13th IEEE Computer Security Foundations Workshop. Los Alamitos: IEEE Computer Society Press, 2000. 24−34.

[19] IEEE Std. 802.11i. Wireless LAN medium access control (MAC) and physical layer (PHY) specifications: medium access control (MAC) security enhancements. 2004.

董玲(1967－),女,湖南攸县人,博士,高级工程师,主要研究领域为信息安全,密码学应用.

陈克非(1959－),男,博士,教授,博士生导师,主要研究领域为密码学,信息安全.

来学嘉(1954－),男,博士,教授,博士生导师,主要研究领域为密码学,信息安全.