安全协议 20 年研究进展*

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)

Twenty Years Development of Security Protocols Research

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@ercist.iscas.ac.cn
http://www.ercist.iscas.ac.cn
Received 2003-02-20; Accepted 2003-07-07

Qing SH. Twenty years development of security protocols research. *Journal of Software*, 2003,14(10): 1740~1752.
http://www.jos.org.cn/1000-9825/14/1740.htm

Abstract: This paper is a survey on the twenty years development of security protocols research. The state of the art in the application of formal methods to the design and analysis of security protocols is presented. Some major threads and emerging trends of research in this area are outlined.
Key words: security protocol; design; analysis; formal methods

摘 要: 总结了安全协议的 20 年研究进展情况,指出形式化方法在安全协议的设计与分析中的重要应用.对安全协议的若干热点研究方向进行了归纳和展望.
关键词: 安全协议;设计;分析;形式化方法
中图法分类号: TP309 **文献标识码**: A

安全协议提供安全服务,是保证网络安全的基础.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,设计一个符合安全目标的安全协议是十分困难的.因此,我们必须借助形式化方法,对安全协议进行设计和分析.自 20 世纪 70 年代末期以来,安全协议的研究已经成为一个热点,有众多的形式化研究方法涌现出来.本文是对这一重要研究领域发展 20 年的简要概括和总结.

本文第 1 节阐述安全协议的背景与基本概念;介绍重要的安全协议;对安全协议发展的 20 年作一简要回顾.第 2 节讨论安全协议的有代表性的形式化分析方法,其中包括基于知识与信念推理的模态逻辑方法、基于定理证明的分析方法、Spi 演算方法等.第 3 节讨论安全协议的设计,其中包括安全协议的设计原则、安全协议的形

* 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.

式描述语言、安全协议的基本假设和针对安全协议的攻击.第 4 节进行展望,讨论安全协议研究领域今后的发展方向.

1 安全协议

1.1 背景与基本概念

安全协议,有时也称作密码协议,是以密码学为基础的消息交换协议,其目的是在网络环境中提供各种安全服务.安全目标是多种多样的.例如,认证协议的目标是认证参加协议的主体的身份.此外,许多认证协议还有一个附加的目标,即在主体之间安全地分配密钥或其他各种秘密.非否认协议的目标有两个:一个是确认发方非否认(non-repudiation of origin),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(non-repudiation of receipt),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、公平性等等.

Needham-Schroeder 协议[1]是最为著名的早期的认证协议,许多广泛使用的认证协议都是以 Needham-Schroeder 协议为蓝本而设计的.Needham-Schroeder 协议可分为对称密码体制和非对称密码体制下的两种版本,分别简称为 NSSK 协议和 NSPK 协议.这些早期的经典安全协议是安全协议分析的“试验床”,亦即每当出现一个新的形式化分析方法,都要先分析这几个安全协议,验证新方法的有效性.同时,学者们也经常以它们为例,说明安全协议的设计原则和各种不同分析方法的特点.

安全协议的设计极易出错,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、符合认证目标的、没有冗余的认证协议也十分困难[2,3].因此,20 年来,为了应对这一挑战,人们设计了不同种类的形式化分析方法,投入了大量的精力,取得了可喜的成果.

安全协议设计与分析的困难性在于:(1) 安全目标本身的微妙性.例如,表面上十分简单的“认证目标”,实际上十分微妙.关于认证性的定义,至今存在各种不同的观点;(2) 协议运行环境的复杂性.实际上,当安全协议运行在一个十分复杂的公开环境时,攻击者处处存在.我们必须形式化地刻画安全协议的运行环境,这当然是一项艰巨的任务;(3) 攻击者模型的复杂性.我们必须形式化地描述攻击者的能力,对攻击者和攻击行为进行分类和形式化的分析;(4) 安全协议本身具有“高并发性”的特点.因此,安全协议的分析变得更加复杂并具有挑战性.

1.2 重要的安全协议

从 1978 年 Needham-Schroeder 协议的诞生算起,安全协议的发展已经历经 20 余年了.

除了 NSSK 协议和 NSPK 协议之外,早期著名的经典安全协议还有 Otway-Rees 协议[4]、Yahlom 协议[5]、大嘴青蛙协议[5]等,以及一些重要的实用协议,如 Keberos 协议[6]、CCITT X.509 协议[7]等.

1997 年,Clark 和 Jacob[8]对安全协议进行了概括和总结,列举了一系列有研究意义和实用价值的安全协议.他们将安全协议进行如下分类:

(1) 无可信第三方的对称密钥协议.属于这一类的典型协议包括以下 ISO 系列协议[9]:ISO 对称密钥一遍单边认证协议、ISO 对称密钥二遍单边认证协议、ISO 对称密钥二遍相互认证协议、ISO 对称密钥三遍相互认证协议、Andrew 安全 RPC 协议[10]等.

(2) 应用密码校验函数(CCF)的认证协议.属于这一类的典型协议包括以下 ISO 系列协议[11]:ISO 应用 CCF 的一遍单边认证协议、ISO 应用 CCF 的二遍单边认证协议、ISO 应用 CCF 的二遍相互认证协议、ISO 应用 CCF 的三遍相互认证协议.

(3) 具有可信第三方的对称密钥协议.属于这一类的典型协议包括 NSSK 协议[1]、Otway-Rees 协议[4]、Yahlom 协议[5]、大嘴青蛙协议[5]、Denning-Sacco 协议[12]、Woo-Lam 协议[13]等.

(4) 对称密钥重复认证协议.属于这一类的典型协议有 Kerberos 协议版本 5、Neuman-Stubblebine 协议[14]、Kao-Chow 重复认证协议[15]等.

(5) 无可信第三方的公开密钥协议.属于这一类的典型协议包括以下 ISO 系列协议[16]:ISO 公开密钥一遍单边认证协议、ISO 公开密钥二遍单边认证协议、ISO 公开密钥二遍相互认证协议、ISO 公开密钥三遍相互认

证协议、ISO 公开密钥二遍并行相互认证协议、Diffie-Hellman 协议[17]等.

(6) 具有可信第三方的公开密钥协议.属于这一类的典型协议有 NSPK 协议[1]等.

1.3 安全协议发展20年的简要回顾

1.3.1 Needham-Schroeder 协议及其改进

NSSK 协议如下所示,其中 A 是发起者,B 是响应者,S 是认证服务器,用于为通信双方之间分配会话密钥.

1. $A \rightarrow S: A, B, N_a$.
2. $S \rightarrow A: \{N_a, B, K_{AB}, \{K_{AB}, A\}_{K_{BS}}\}_{K_{AS}}$.
3. $A \rightarrow B: \{K_{AB}, A\}_{K_{BS}}$.
4. $B \rightarrow A: \{N_b\}_{K_{AB}}$.
5. $A \rightarrow B: \{N_b - 1\}_{K_{AB}}$.

在协议的第 1 步,A 向 S 发送 A,B 和临时值 N_a.第 2 步,S 生成 A 和 B 之间的会话密钥 K_{AB},并向 A 发送 N_a,B 和 K_{AB} 以及用 S 和 B 之间的共享密钥 K_{bs} 加密的证书 $\{K_{AB}, A\}$.第 3 步,A 向 B 转发这个证书.第 4 步,B 解密这个证书,得到 K_{AB},并用它加密临时值 N_b 之后发送给 A.第 5 步,A 向 B 发送用 K_{AB} 加密的 N_b −1.这里,N_b −1 可用任何一个 N_b 的函数代替,表示这一消息来自 A,并非来自 B.

NSPK 协议如下:

1. $A \rightarrow B: \{N_a, A\}_{K_B}$.
2. $B \rightarrow A: \{N_a, N_b\}_{K_A}$.
3. $A \rightarrow B: \{N_b\}_{K_B}$.

协议假定双方都知道对方的公开密钥.A 首先生成临时值 N_a,与其标识符级连,用 B 的公开钥加密后发送给 B.B 生成临时值 N_b,与 N_a 级连后用 A 的公开钥加密后发送给 A.因此,B 通过证明 B 能读第 1 条消息从而响应了发起者的请求.最后,A 返回用 B 的公开钥加密的 N_b.该协议的目标是,双方可以共享值 N_a 与 N_b,每一方都将这些值与对方相结合,没有第三方可以掌握它们.例如,这个协议可以用于以下场合,即这两个值一起散列后,生成一个共享的对称密钥,作为一次会话密钥应用.

NSSK 协议和 NSPK 协议自问世以来,受到了广泛的关注.BAN 逻辑以 NSSK 协议和 NSPK 协议为试验床,对它们进行了分析.

对 NSSK 协议最为著名的攻击是 Denning-Sacco 攻击[12].Denning 和 Sacco 认为,NSSK 协议的主要安全问题在于响应者 B 无法确定消息 3 的新鲜性.攻击者可以破译密钥,并重放消息 3 给 B,然后完成整个协议.Denning 和 Sacco 建议应用时间戳修改 NSSK 协议,修改后的 Denning-Sacco 协议如下:

1. $A \rightarrow S: A, B$.
2. $S \rightarrow A: \{B, K_{AB}, T, \{A, K_{AB}, T\}_{K_{BS}}\}_{K_{AS}}$.
3. $A \rightarrow B: \{A, K_{AB}, T\}_{K_{BS}}$.

其中,T 是时间戳.在上述协议中,响应者 B 可以验证消息 3 的新鲜性.因此,Denning-Sacco 协议不需要 NSSK 协议中的第 4 和第 5 条消息.

1990 年,Boyd[18]通过实例指出,如果应用序列密码,则在 NSSK 协议中,密文消息 4 与 5 之间的差别只有 1 个比特,协议极易受到攻击.

针对 NSPK 协议的最有名的攻击来自 Lowe[19].Lowe 指出,NSPK 协议的主要安全缺陷在于其中的消息 2.由于消息中没有 B 的标识符,攻击者可以假冒 B 的身份发送消息 2.Lowe 改进后的 NSPK 协议如下:

1. $A \rightarrow B: \{N_a, A\}_{K_B}$.
2. $B \rightarrow A: \{B, N_a, N_b\}_{K_A}$.
3. $A \rightarrow B: \{N_b\}_{K_B}$.

从 1978 年 NSPK 协议问世以来,到 Lowe 于 1996 年发现 NSPK 协议的安全缺陷,已经过去了大约 17 年之久.安全协议设计的困难性和安全协议分析的微妙性,由此可见一斑.

1.3.2 Dolev-Yao 模型

1983 年,Dolev 和 Yao 发表了安全协议发展史上的一篇重要的论文[20].该论文的主要贡献有两点.其一是将安全协议本身与安全协议所具体采用的密码系统分开,在假定密码系统是"完善"的基础上讨论安全协议本身的正确性、安全性、冗余性等课题.从此,学者们可以专心研究安全协议的内在安全性质了.亦即,问题很清楚地被划分为两个不同的层次:首先研究安全协议本身的安全性质,然后讨论实现层次的具体细节,包括所采用的具体密码算法等等.

第 2 点贡献是,Dolev 和 Yao 建立了攻击者模型.他们认为,攻击者的知识和能力不能够低估,攻击者可以控制整个通信网络.Dolev 和 Yao 认为攻击者具有如下能力:(1) 可以窃听所有经过网络的消息;(2) 可以阻止和截获所有经过网络的消息;(3) 可以存储所获得或自身创造的消息;(4) 可以根据存储的消息伪造消息,并发送该消息;(5) 可以作为合法的主体参与协议的运行.

Dolev 和 Yao 的工作具有深远的影响.迄今为止,大部分有关安全协议的研究工作都遵循 Dolev 和 Yao 的基本思想.

1.3.3 BAN 逻辑

BAN 逻辑[5]开创了安全协议形式化分析的先河,是一项开拓性的工作.BAN 逻辑简单、实用,抽象程度高,可以揭示安全协议中的安全缺陷与冗余性.例如,BAN 逻辑分析发现了 CCITT X.509 标准[7]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:第一,BAN 逻辑不区分看见一条消息和理解一条消息;第二,BAN 逻辑的信念演化过程是单调递增的;第三,BAN 逻辑不讨论 trust;第四,BAN 逻辑不讨论知识;第五,BAN 逻辑假设参加协议的主体是诚实的,他们都忠诚地根据协议的法则执行协议;第六,BAN 逻辑假设加密系统是完善的(perfect)等等.

但是,BAN 逻辑的简单性也为 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实现保密性质和认证性质两个重要目标.

1990 年,Nessett[21]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. $B \to A: \{N_b\}_{K_{AB}}$.

Nessett 用 BAN 逻辑分析上述协议,得出 K_{AB} 是良好的会话密钥这一结论.但是,任何主体都可以通过 A 的公开密钥获得 K_{AB}.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的问题,亦即,未考虑保密性的问题.

BAN[22]对 Nessett 的批评答复如下:在 BAN 逻辑的论文中已经清楚地说明,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 $A \xleftarrow{K_{AB}} B$ 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.

1.3.4 CSP 方法与模型校验技术

1996 年,Lowe[19]首先采用 CSP(通信顺序进程)方法和模型校验技术对安全协议进行形式化分析.他应用 CSP 模型和 CSP 模型校验工具 FDR 分析 NSPK 协议,并令人惊讶地发现了一个近 17 年来未知的攻击.Lowe 的论文发表不久,Roscoe[23]对 CSP 和 FDR 的组合作了进一步的研究.他们认为,CSP+FDR 是形式化分析安全协议

的一条新途径.

模型校验技术是验证有限状态系统的自动化分析技术,是一种安全协议的自动验证工具.Lowe 等学者应用 CSP 方法的成功,促进了这一领域的发展.Schneider[24~26]发表了一系列关于 CSP 方法应用的论文,应用 CSP 方法讨论安全协议的安全性质、匿名等问题;分析了各种安全协议,例如 NSPK 协议、非否认协议等.

美国卡内基-梅隆大学以 Clarke 教授为首的研究小组,长期从事定理证明和自动校验的研究.他们提出了一种通用的模型校验器,构造了一种新型的模型及其代数理论,并证明了该模型的有效性.Marrero,Clarke 和 Jha[27]应用该方法对 NSPK 协议进行分析,得到了与 Lowe 相同的结论[19].

Mitchell[28]的方法是通过状态计数工具 Murphi 分析安全协议,从安全协议可能到达的状态,分析安全协议是否安全.他应用 Murphi 分析了一系列著名的安全协议,成功地发现了所有已知的攻击.

1.3.5 串空间方法

Thayer,Herzog 和 Guttman[29~31]提出了串空间(strand space)模型,这是一种结合定理证明和协议迹的混合方法.事实证明,串空间模型是分析安全协议的一种实用、直观和严格的形式化方法.

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于另一个串的接收消息.从(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.从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.

Thayer,Herzog 和 Guttman 应用串空间模型,分析了多个经典安全协议,成功地找到目前已经发现的攻击.

Perrig 和 Song[32]等人对串空间模型进行了重要的扩展,将其增强和优化,并将串空间模型推广到分析三方安全协议.Song[33]应用串空间模型,研制出安全协议自动检验工具——Athena.Athena 结合定理证明和模型校验技术,证明从一些初始状态开始,进行回退搜索.初始状态是满足某种安全属性的丛.

1.3.6 安全协议目标的讨论

关于协议安全目标最早的讨论源于 1993 年 van Oorschot 的工作[34].van Oorschot 给出了关于认证协议的 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.

(G2) 实体认证:

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

A 不仅认证 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:

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

这里,$A \xleftrightarrow{K-} B$ 表示 K 是 A 的适用于 B 的未经确认的密钥.除了 A 和 B 之外,任何其他主体都不知道也不能推导出 K.G3 说明,A 相信除了 B 之外,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.

(G4) 密钥确认:

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

这里,$A \xleftrightarrow{K+} B$ 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.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.

(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.

1996 年,Gollmann[35]正式提出讨论认证协议的目标,其论文的题目就是"实体认证的含义是什么?".关于安全目标的进一步讨论,可参见文献[19,35,36].

2 安全协议的形式化分析

2.1 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最直接、最简单的一种方法.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.Syverson[37]阐述了在安全协议的分析中,知识、信念和语义之间的关系与相互作用.

在这类方法中,最著名的是 BAN 类逻辑,其中包括 BAN 逻辑[5]、GNY 逻辑[38]、AT 逻辑[39]、VO 逻辑[34]和 SVO 逻辑[40].其他相近的工作还包括:Bieber 逻辑——CKT5[41];Syverson 逻辑——KPL[42];Rangan 逻辑[43];Moser 逻辑[44];Yahalom,Klein 和 Beth 的 YHK 逻辑[45];Kessler 和 Wedel 的 AUTOLOG 逻辑[46]等.1999 年,Kindred 在他的博士论文[47]中提出了密码协议的生成理论——RV 逻辑,是这方面的又一个新成果.

BAN 逻辑问世后,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.并且,若 $\frac{C_1}{C_2}$ 是逻辑公设,则对任何主体 P,$\frac{P|\equiv C_1}{P|\equiv C_2}$ 也是逻辑公设.

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;(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 逻辑的分析中,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.

GNY 逻辑的缺点是过于复杂,因此不实用.但是,它仍然在安全协议 20 年的发展史中占有重要的地位.GNY 逻辑的出现,使我们对 BAN 逻辑有了更加深刻的认识.

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,并获得相近的结论.但是,GNY 得到的是一个更加复杂的逻辑.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中不必要的混和;(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,即 Modus Ponens 规则和 Necessitation 规则.

VO 逻辑的贡献则是扩展了 BAN 逻辑的应用范围.Diffie-Hellman 协议[17]是许多近代密钥分配协议的基础,VO 逻辑的设计目标之一就是增加分析 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[48]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 6 种不同形式的认证目标.

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 逻辑对一些概念作了有别于 AT 逻辑的重新定义,从而取消了 AT 逻辑系统中的一些限制.

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:

(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.

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[49,50].

2.2 基于定理证明的分析方法

这种方法可以分为两类,一类是推理构造方法,另一类是证明构造方法.在推理构造方法中,重要的工作包括:(1) Meadows 的 NRL 协议分析器方法[51].它发现了许多已知的和未知的安全协议漏洞,并成功地用于分析 IETF 标准——因特网密钥交换协议 IKE[52];(2) Cervesato 等学者的基于线性逻辑的协议验证方法[53];(3) Millen 等学者的基于逻辑规则的协议验证方法[54].推理构造方法的优点是可以发现攻击,并可以证明协议在多回合运行下的正确性.其缺点是需要用户介入,防止状态爆炸.

Kemmerer 等学者研制的 Ina Jo 和 ITP 是证明构造方法的典型代表[55].这一领域的另一项重要工作是 Paulson 的基于归纳的定理证明方法[56,57].他研制的定理证明器 Isabelle 可以应用归纳方法分析安全协议.Thayer,Herzog 和 Guttman 随后提出的串空间模型,在很多方面继承和发扬了 Paulson 方法的基本思想.证明构造方法的优点是可以分析无限大小的协议,不限制主体参与协议运行的回合.其缺点是证明过程不能全部自动化,需要人工进行“专家式”的干预,在使用范围上受到一定的限制.

2.3 Spi演算方法

1997 年,Abadi 和 Gordon 在 Pi 演算[58]的基础上建立了 Spi 演算[59]方法.这种方法根据 Dolev-Yao 模型,假定协议执行的每一步都可能与攻击者的执行步骤交叉.Pi 演算是并发计算的基础,它引入了通道和作用域的概念.由于作用域之外的进程不能访问通道,在一定程度上保证了通道通信的安全性.Spi 演算对 pi 演算进行了增强与扩充,增加了支持密码系统的原语,使 Spi 演算可以描述基于密码系统的安全协议.

除了 Abadi 和 Gordon 的研究之外,应用 Spi 演算分析安全协议的重要工作还有文献[60~62].Amadio 和 Lugiez[60]应用 Spi 演算方法分析对称密钥安全协议;Abadi 和 Blanchet[61]应用 Spi 演算方法分析公开密钥安全协议;Amadio 和 Prasad[62]在应用 Spi 演算方法分析时,对攻击者的消息构造能力进行了刻画和限制.

目前,针对 Spi 演算的研究主要集中在以下两个方面:一方面对 Spi 演算进一步扩展,扩大它的应用范围;另一方面.进一步研究 Spi 演算的语义,为安全协议的分析提供更为坚实的基础.

3 安全协议的设计

在安全协议发展的 20 年历史中,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[63~65].

3.1 安全协议的设计原则

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,我们可以提出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,以降低成本,扩大应用范围.

第(7)条十分重要."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.有关安全协议设计原则的进一步讨论,参见文献[66].

3.2 安全协议的形式描述语言

设计安全协议,需要协议本身的形式描述规范.早期有代表性的描述安全协议的形式语言有 Lotos[67]和 Ina Jo[55]等.

Lotos 是基于 CCS 的标准化语言,由两部分组成,其中一部分描述抽象数据类型和密码操作,另一部分描述协议的实体行为.1991 年,Lotos 成为 ISO 标准,随后出现了扩展版本 E-Lotos.Ina Jo 基于通信有限状态机的语言,它与 Lotos 不同,用传统的形式规范语言描述安全协议.

为了统一安全协议描述的标准,出现了以 CASPL[68]为代表、通用性较强的描述安全协议的形式语言.安全协议分析软件 Interrogator[54]率先应用了早期版本的 CASPL 语言.当前版本的 CASPL 语言提供通用的描述格式,应用 Lex 和 Yacc 描述词法和语法,可以自动地分析安全协议格式,具有描述安全目标的能力.

3.3 安全协议的基本假设

在设计安全协议时,必须注意对安全协议所作的基本假设.例如:

(1) 密文块不能被篡改,也不能用几个小的密文块组成一个新的大密文块;

(2) 一条消息中的两个密文块被视为分两次分别到达;

(3) 密码系统是完善的(perfect),即只有掌握密钥的主体才能理解密文消息;

(4) 无加密项冲突,即若有 $\{m_1\}_{K_1}=\{m_2\}_{K_2}$,则一定有 $m_1=m_2, K_1=K_2$;

(5) 参与协议的主体包含诚实的合法用户和攻击者.合法用户将遵循协议的规定执行协议.攻击者也可以是系统的合法用户,但他不会完全遵守协议.

3.4 针对安全协议的攻击

在设计安全协议时,必须对攻击对手有全面和深刻的认识.所设计的安全协议至少应当能够抵抗已知的各种攻击.

3.4.1 攻击者的知识和能力

Dolev-Yao 模型认为,攻击者可以控制整个通信网络,并应当假定攻击者具有相应的知识与能力.例如,我们应当假定,攻击者除了可以窃听、阻止、截获所有经过网络的消息等之外,还应具备以下知识和能力:(1) 熟悉加解、解密、散列(hash)等密码运算,拥有自己的加密密钥和解密密钥;(2) 熟悉参与协议的主体标识符及其公钥;(3) 具有密码分析的知识和能力;(4) 具有进行各种攻击,例如重放攻击的知识和能力.

3.4.2 重放攻击

重放攻击是最基本、最常用、危害性最大的一种攻击形式.Syverson[69]对重放攻击进行了分类,如下所示:

A. 当前回合外攻击	B. 当前回合内攻击
1. 交错攻击	
(a) 偏转攻击	(a) 偏转攻击
(i) 反射攻击	(i) 反射攻击
(ii) 指向第三方的偏转攻击	(ii) 指向第三方的偏转攻击
(b) 直接重放攻击	(b) 直接重放攻击
2. 经典重放攻击	
(a) 偏转攻击	
(i) 反射攻击	
(ii) 指向第三方的偏转攻击	
(b) 直接重放攻击	

基于重放发生在什么回合,可以将重放攻击分为两类:

(A) 在当前回合外攻击中,重放的消息来自协议当前回合之外,因此至少涉及协议的两个回合运行,可以并发也可以顺序地实现.

(1) 交错攻击需要两回合或多回合同时执行协议,著名的例子是 Lowe[19]对 NSPK 协议的攻击.

(2) 经典重放也涉及当前回合外执行协议,但不要求同时执行协议.攻击者存储在前面的回合中传送的消息,并抓住机会重放它们,对协议的当前回合进行攻击.Denning 和 Sacco[12]对 NSSK 协议的攻击就是经典重放的一个著名例子.

(B) 在当前回合内攻击中,重放的消息来自协议当前回合.关于当前回合内攻击的例子,参见文献[70,71].

另外一种重放攻击的分类法考察攻击者对消息重定向的方法,这种分类法称为目的地分类法[69].分类如下:

(a) 偏转重放攻击.重放消息重新定向,发送给不同于原接收者的第三方.这种情形可以进一步分为如下子类:

(i) 重放消息重定向,发送给原发送者,称为反射重放攻击.

(ii) 重放消息重定向,发送给第三方,即不同于原发送者和原接收方的第三方.

(b) 攻击者通过延时的方法(可能涉及不同的协议回合),将消息传送给目的地,称为直接重放攻击.

关于其他各种攻击形式与重放攻击的进一步讨论,参见文献[3,8,72].

3.4.3 串空间中的攻击者模型

根据 Dolev-Yao 模型,不同的形式化方法对攻击者能力的处理方法也有所不同.在串空间模型中,对攻击者进行如下的形式化刻画.攻击者具有 6 种基本能力,用下述攻击者迹的集合表示.

(1) M. 正文消息:$\langle +t\rangle$,其中 $t\in T$,T 表示正文消息集合.

(2) K. 密钥:$\langle +k\rangle$,其中 $k\in k_p$,k_p 表示攻击者所拥有的密钥集合.

(3) C. 并置:$\langle -g,-h,+gh\rangle$;

(4) S. 分解:$\langle -gh,+g,+h\rangle$;

(5) E. 加密:$\langle -k,-h,+\{h\}_k\rangle$;

(6) D. 解密:$\langle -k^{-1},-\{h\}_k,+h\rangle$.

4 展 望

20 年来,安全协议研究的进展十分可喜,取得了丰富的研究成果.特别是 20 世纪 90 年代以来,研究取得突破性进展,对安全协议若干本质性的问题有了更为深刻的认识.

但是,这一领域还有许多问题有待解决.Meadows[73]提出了安全协议领域的若干公开问题.电子商务,特别是非否认与公平交换,是另一个重要的协议及形式化分析领域,在公平交易中,协议本身并没有对立面,我们关心的是公平性.在非否认协议中,协议目标是获得主体所不能否认的证据.显然,非否认性与公平性是密切相关的.最初涉及这个领域的是 Kailar 逻辑[74~76].Kailar 逻辑是 BAN 类逻辑的进一步发展.关于安全协议的设计与逻辑分析,文献[77]有详尽的分析,可供参考.

我们认为,这一领域中可能的热点研究方向包括:(1) 减少对协议所作的基本假设,例如“完善”的密码系统假设、自由加密假设等,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.(7) 在模型校验等方法中,解决“状态爆炸”的问题.(8) 新领域的研究,例如拒绝服务(DOS)模型的研究等.

References:

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

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

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

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

[5] Burrows M, Abadi M, Needham R. A logic of authentication. In: Proceedings of the Royal Society of London A, Vol 426. 1989. 233~271.

[6] Miller SP, Neuman C, Schiller JI, Saltzer JH. Kerberos authentication and authorization system. Project Athena Technical Plan Section E.2.1, MIT, 1987.

[7] CCITT. CCITT draft recommendation X.509. The Directory-Authentication Framework, Version 7, 1987.

[8] 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.

[9] ISO/IEC. Information technology—security techniques—entity authentication mechanisms part 2: Entity authentication using symmetric techniques. 1993.

[10] Satyanarayanan M. Integrating security in a large distributed system. Technical Report, CMU-CS, CMU, 1987. 87~179.

[11] ISO/IEC. Information technology—security techniques—entity authentication mechanisms part 4: Entity authentication using cryptographic check functions. 1993.

[12] Denning D, Sacco G. Timestamps in key distribution protocols. Communications of the ACM, 1981,24(8):533~536.

[13] Woo T, Lam S. A lesson on authentication protocol design. Operating Systems Review, 1994,28(3):24~37.

[14] Neuman BC, Stubblebine SG. A note on the use of timestamps as nonces. Operating Systems Review, 1993,27(2):10~14.

[15] Kao IL, Chow R. An efficient and secure authentication protocol using uncertified keys. Operating Systems Review, 1995,29(3): 14~21.

[16] ISO/IEC. Information technology—security techniques—entity authentication mechanisms part 3: Entity authentication using a public key algorithm. 1995.

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

[18] Boyd C. Hidden assumptions in cryptographic protocols. Proceedings of the IEE, 1990,137(6):433~436.

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

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

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

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

[23] Roscoe A, Goldsmith M. The perfect ‘spy’ for model-checking cryptoprotocols. In: DIMACS Workshop on Design and Formal Verification of Security Protocols. 1997.

[24] Schneider SA. Using CSP for protocol analysis: The Needham-Schroeder public-key protocol. Technical Report, CSD-TR-96-14, Royal Holloway: University of London, 1996.

[25] Schneider SA. Security properties and CSP. In: Proceedings of the 1996 IEEE Symposium on Security and Privacy. Los Alamitos: IEEE Computer Society Press, 1996. 174~187.

[26] Schneider S, Sidiropoulos A. CSP and anonymity. In: Proceedings of Computer Security-ES-ORICS 96. Berlin: Springer-Verlag, 1996. 198~218.

[27] Marrero W, Clarke E, Jha S. A model checker for authentication protocols. In: DIMACS Workshop on Design and Formal Verification of Security Protocols. 1997.

[28] Mitchell J, Mitchell M, Stern U. Automated analysis of cryptographic protocols using murphi. In: Proceedings of the 1997 IEEE Computer Society Symposium on Research in Security and Privacy. Los Alamitos: IEEE Computer Society Press, 1997. 141~151.

[29] 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.

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

[31] 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.

[32] Perrig A, Song D. Looking for diamonds in the desert-extending automatic protocol generation to three-party authentication and key agreement. In: Proceedings of the 13th IEEE Computer Security Foundations Workshop. Los Alamitos: IEEE Computer Society Press, 2000. 64~76.

[33] Song D. Athena: A new efficient automatic checker for security protocol analysis. In: Proceedings of the 1999 IEEE Computer Security Foundations Workshop. Los Alamitos: IEEE Computer Society Press, 1999. 192~202.

[34] 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.

[35] 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.

[36] 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.

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

[38] 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.

[39] 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.

[40] 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.

[41] 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.

[42] 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.

[43] 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.

[44] 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.

[45] 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.

[46] Kessler V, Wedel G. AUTOLOG—An advanced logic of authentication. In: Proceedings of the Computer Security Foundations Workshop. Los Alamitos: IEEE Computer Society Press, 1994. 90~99.

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

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

[49] 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.

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

[51] Meadows C. The NRL protocol analyzer: An overview. Journal of Logic Programming, 1996,26(2):113~131.

[52] Meadows C. Analysis of the Internet key exchange protocol using the NRL protocol analyzer. In: Proceedings of the IEEE Symposium on Security and Privacy. Los Alamitos: IEEE Computer Society Press, 1999. 84~89.

[53] Cervesato I, Durgin N, Lincoln P, Mitchell J. A meta-notation for protocol analysis. In: Proceedings of the 1999 IEEE Symposium on Security and Privacy. Los Alamitos: IEEE Computer Society Press, 1999. 55~69.

[54] Millen J. The Interrogator model. In: Proceedings of the 1995 IEEE Symposium on Security and Privacy. Los Alamitos: IEEE Computer Society Press, 1995. 251~260.

[55] Kemmerer R, Meadows C, Millen J. Three systems for cryptographic protocol analysis. Journal of Cryptology, 1994,7(2):251~260.

[56] Paulson LC. Mechanized proofs for a recursive authentication protocol. In: Proceedings of the 10th IEEE Computer Security Foundations Workshop. Los Alamitos: IEEE Computer Society Press, 1997. 84~94.

[57] Paulson LC. The inductive approach to verifying cryptographic protocols. Journal of Computer Security, 1998,(6):85~128.

[58] Milner R, Parrow J, Walker D. A calculus of mobile processes. Information and Computation, 1992,100(1):1~77.

[59] Abadi M, Gordon AD. A calculus for cryptographic protocols: The spi calculus. In: Proceedings of the 4th ACM Conference on Computer and Communications Security. 1997. 36~47.

[60] Amadio R, Lugiez D. On the reachability problem in cryptographic protocols. In: Proceedings of the CONCUR. Berlin: Springer-Verlag, 2000. 380~394.

[61] Abadi M, Blanchet B. Secrecy types for asymmetric communication. In: Proceedings of Foundations of the Software Science and Computation Structures. 2001. 35~49.

[62] Amadio R, Prasad S. The game of the name in cryptographic tables. In: Proceedings of the ASIAN'99. Berlin: Springer-Verlag, 1999. 15~26.

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

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

[65] 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.

[66] Abadi M, Needham R. Prudent engineering practices for crypto-graphic protocols. In: Proceedings of the 1994 IEEE Symposium on Security and Privacy. Los Alamitos: IEEE Computer Society Press, 1994. 122~136.

[67] Bolognesi T, Brinksma E. Introduction to the ISO specification language LOTOS. Computer Networks and ISDN Systems, 1987,14: 25~59.

[68] Millen JK. CAPSL: Common authentication protocol specification language. Technical Report, MP 97B48, The MITRE Corporation, 1997.

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

[70] Syverson P. On key distribution protocols for repeated authentication. Operating Systems Review, 1993,27(4):24~30.

[71] Carlsen U. Using logics to detect implementation-dependent flaws. In: Proceedings of the 9th Annual Computer Security Applications Conference. Los Alamitos: IEEE Computer Society Press, 1993. 64~73.

[72] 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).

[73] Meadows C. Open issues in formal methods for cryptographic protocol analysis. In: Proceedings of the DARPA Information Survivability Conference and Exposition. Los Alamitos: IEEE Computer Society Press, 2000. 237~250.

[74] Kailar R. Reasoning about accountability in protocols for electronic commerce. In: Proceedings of the IEEE Symposium on Security and Privacy. Los Alamitos: IEEE Computer Society Press, 1995. 236~250.

[75] Zhou DC, Qing SH, Zhou ZF. Limitations of Kailar logic. Journal of Software, 1999,10(12):1238~1245 (in Chinese with English abstract).

[76] Zhou DC, Qing SH, Zhou ZF. A new approach for the analysis of electronic commerce protocols. Journal of Software, 2001,12(9): 1318~1328 (in Chinese with English abstract).

[77] Qing SH. Design and logical analysis of security protocols. Journal of Software, 2003,14(7):1300~1309 (in Chinese with English abstract).

附中文参考文献:

[2] 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.

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

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

[72] 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.

[75] 周典萃,卿斯汉,周展飞.Kailar 逻辑的缺陷.软件学报,1999,10(12):1238~1245.

[76] 周典萃,卿斯汉,周展飞.一种分析电子商务协议的新工具.软件学报,2001,12(9):1318~1328.

[77] 卿斯汉.安全协议的设计与逻辑分析.软件学报,2003,14(7):1300~1309.

敬 告 作 者

《软件学报》创刊以来,蒙国内外学术界厚爱,收到许多高质量的稿件,其中不少在发表后读者反映良好,认为本刊保持了较高的学术水平.但也有一些稿件因不符合本刊的要求而未能通过审稿.为了帮助广大作者尽快地把他们的优秀研究成果发表在我刊上,特此列举一些审稿过程中经常遇到的问题,请作者投稿时尽量予以避免,以利大作的发表.

1. 读书偶有所得,即匆忙成文,未曾注意该领域或该研究课题国内外近年来的发展情况,不引用和不比较最近文献中的同类结果,有的甚至完全不列参考文献.

2. 做了一个软件系统,详尽描述该系统的各个方面,如像工作报告,但采用的基本上是成熟技术,未与国内外同类系统比较,没有指出该系统在技术上哪几点比别人先进,为什么先进.一般来说,技术上没有创新的软件系统是没有发表价值的.

3. 提出一个新的算法,认为该算法优越,但既未从数学上证明比现有的其他算法好(例如降低复杂性),也没有用实验数据来进行对比,难以令人信服.

4. 提出一个大型软件系统的总体设想,但很粗糙,而且还没有(哪怕是部分的)实现,很难证明该设想是现实的、可行的、先进的.

5. 介绍一个现有的软件开发方法,或一个现有软件产品的结构(非作者本人开发,往往是引进的,或公司产品),甚至某一软件的使用方法.本刊不登载高级科普文章,不支持在论文中引进广告色彩.

6. 提出对软件开发或软件产业的某种观点,泛泛而论,技术含量少.本刊目前暂不开办软件论坛,只发表学术文章,但也欢迎材料丰富,反映现代软件理论或技术发展,并含有作者精辟见解的某一领域的综述文章.

7. 介绍作者做的把软件技术应用于某个领域的工作,但其中软件技术含量太少,甚至微不足道,大部分内容是其他专业领域的技术细节,这类文章宜改投其他专业刊物.

8. 其主要内容已经在其他正式学术刊物上或在正式出版物中发表过的文章,一稿多投的文章,经退稿后未作本质修改换名重投的文章.

本刊热情欢迎国内外科技界对《软件学报》踊跃投稿.为了和大家一起办好本刊,特提出以上各点敬告作者.并且欢迎广大作者和读者对本刊的各个方面,尤其是对论文的质量多多提出批评建议.