Kailar逻辑的缺陷*

周典萃 卿斯汉 周展飞

(中国科学院软件研究所 北京 100080)
(中国科学院信息安全技术工程研究中心 北京 100080)

摘要 近年来,电子商务协议的设计逐渐成为热点.可追究性是指电子商务协议迫使个人或组织对自己在电子交易中的行为负责的能力.缺乏可追究性,电子交易容易引起争议.因此,Rajashekar Kailar提出了一种用于分析电子商务协议中可追究性的形式化分析方法,简称Kailar逻辑.该文指出这一逻辑的缺陷:(1) 不能分析协议的公平性;(2) 对协议语句的解释及初始化假设是非形式化的,存在局限性;(3) 无法处理密文.

关键词 可追究性,电子商务,协议,协议分析.

中图法分类号 TP309

随着计算机及计算机网络技术的发展,社会各行业越来越依赖计算机来进行数据处理和信息交换.近年来,基于远程网(如Internet)的网上交易,即电子商务的研究开发更是进行得如火如荼.电子商务巨大的市场应用前景使得一些著名的计算机公司和金融机构将它立为一个重要的研究课题,以期在此领域取得领先地位.借助于远程网,电子商务可以使商家拥有更大的用户群,同时也使远程商业交易变得更为方便、快捷,从而大大提高了人们生活和工作的效率.尽管电子商务的应用前景十分诱人,但人们对电子商务的安全却普遍心存疑虑.密码学为电子商务的安全提供了有效的保障,如何用密码技术来解决电子商务中存在的安全性问题则是电子商务研究所面临的主要课题.

在现实的商业交易活动中,人们常常借助于票证(如合同、发票等)来解决交易中出现的争议和纠纷.票证的不易伪造性使得交易的双方无法否认自己在交易中的行为,从而为解决交易中的纠纷提供了一种有效的途径.同样地,作为电子交易规则的电子商务协议也必须具备这一机制,它必须能够为交易双方提供足够的证据,以便在产生纠纷时,仲裁机构可以利用这些证据来解决纠纷,即电子商务协议的设计必须满足可追究性原则.

与现实的交易活动有所不同,在电子交易中传输的消息极易被伪造,因而无法起到票证的作用.数字签名技术使得电子交易不易被伪造,而且人们可以验证其来源.它在电子商务协议中的应用解决了电子交易中传输的消息易被伪造产生的问题.

但是,一个安全强度较高的密码算法并不能保证电子商务满足可追究性的要求,电子商务协议是否遵循可追究性原则不仅依赖于所用密码的安全强度,还与协议的自身结构有着密切的联系.

通过对认证协议的研究,我们可以发现,密码协议的一些微小改动都会导致协议的安全漏洞,同时我们又很难察觉这些安全漏洞.鉴于此,可否通过严格的形式化方法来验证电子商务协议的安全性成为电子商务研究中亟待解决的一个问题.

1989年,Burrows等人[1]提出一种基于信念逻辑的形式化方法,用于分析认证协议的安全性.此后,研究人员对这种方法进行了大量的改进和扩充,形成了所谓的BAN(即Michael Burrows, Martin Abadi和Roger Need-

* 本文研究得到国家自然科学基金资助.作者**周典萃**,1971年生,硕士,主要研究领域为信息安全基础理论.**卿斯汉**,1939年生,研究员,博士生导师,主要研究领域为信息安全理论和技术.**周展飞**,1969年生,博士后,主要研究领域为密码理论,应用数学.

本文通讯联系人:卿斯汉,北京 100080,中国科学院软件研究所

本文1999-02-08收到原稿,1999-05-25收到修改稿

ham)类逻辑.那么,我们是否可以借助于信念逻辑来验证电子商务协议的可追究性呢?通过认证协议和电子商务协议的比较,Kailar[2]指出了大家熟知的 BAN 类逻辑不适于分析电子商务协议的根本原因在于,信念逻辑是要证明某个主体相信某一公式,而可追究性的目的在于某个主体要向第三方证明另一方对某个公式负有责任.为此,Kailar 提出了新的逻辑,用于分析电子商务协议的可追究性.

本文着重分析 Kailar 逻辑的缺陷及其应用的局限性.这也许可以为我们改进电子商务协议的形式化分析工具提供一些借鉴.

1 Kailar 逻辑

在介绍 Kailar 逻辑[2]之前,先列举本文中用到的基本符号.

$A,B,\ldots$:参与协议的各个主体.

m:消息,由一个主体发送给另一个主体的消息.

TTP:可信任第三方(trusted third party,简称 TTP).

K_a:A 的公开钥,用于验证 A 的数字签名.K_a^{-1} 是与 K_a 对应的 A 的私有密钥.

k:会话密钥.

K_{ab}:A 与 B 的共享密钥.

Kailar 逻辑的公式如下:

A CanProve x:对于任何主体 B,A 能执行一系列操作使得通过这些操作以后,A 能使 B 相信公式 x,而不泄漏任何秘密 $y(y\neq x)$给 B.

K_a Authenticates A:K_a 能用于验证 A 的数字签名.

x in m:x 是 m 中的一个或几个可被理解的域,它的含义是由协议设计者明确定义的.可被理解的域通常是明文或者主体拥有密钥的加密域.

A Says x:A 声明公式 x 并对 x 以及 x 能推导出的公式负责.通常,隐含地假设以下推论成立.

$$A \text{ Says } (x,y)\Rightarrow A \text{ Says } x.$$

A Receives m SignedWith K^{-1}:A 收到一个用 K^{-1} 签名的消息 m.通常,隐含地假设以下推论成立,

$$\frac{A \text{ Recieves } m \text{ SignedWith } K^{-1};x \text{ in } m}{A \text{ Recieves } x \text{ SignedWith } K^{-1}}.$$

A IsTrustedOn x:A 对公式 x 具有管辖权,即 A 被协议其他主体所相信 A 声明的公式 x 是正确的.

推理规则如下.

连接:
$$\frac{A \text{ CanProve } x;\ A \text{ CanProve } y}{A \text{ CanProve } (x\wedge y)},$$
如果 A 能够证明公式 x,并且 A 能够证明公式 y,那么 A 能够证明公式 $x\wedge y$.

推理:
$$\frac{A \text{ CanProve } x;x\Rightarrow y}{A \text{ CanProve } y},$$
如果 A 能够证明公式 x,而由公式 x 能推导公式 y(即公式 x 蕴涵有公式 y 的含义),那么 A 能够证明公式 y.

签名:
$$\frac{A \text{ Receives } (m \text{ SignedWith } K^{-1});\ x \text{ in } m;\ A \text{ CanProve } (K \text{ Authenticates } B)}{A \text{ CanProve } (B \text{ Says } x)},$$
如果 A 收到一个用私钥 K^{-1} 签名的消息 m,m 中包含 A 能理解的公式 x,并且 A 能够证明公钥 K 能用于验证 B 的签名,那么 A 能证明 B 声明了公式 x.

信任:
$$\frac{A \text{ CanProve } (B \text{ Says } x);\ A \text{ CanProve } (B \text{ IsTrustedOn } x)}{A \text{ CanProve } x},$$
如果 A 能够证明 B 对 x 有管辖权,并且 B 声明了公式 x,那么 A 能证明公式 x.

利用 Kailar 逻辑来分析协议共有 4 个步骤:

(1) 列举协议要达到的目标.

(2) 对协议的语句进行解释,使之转化为逻辑公式.在这一步中,只对那些包含签过名的明文消息并且和分析可追究性相关的语句进行解释.

(3) 列举分析协议时需要用到的初始假设.

(4) 对协议进行分析.

2 Kailar 逻辑的缺陷

本节将通过实例说明 Kailar 逻辑中存在的缺陷.

2.1 基于公钥体制的 IBS 协议

可追究性原则要求电子商务协议为参与协议的各个主体提出充分的证据以解决今后可能出现的纠纷.但电子商务协议的安全仅满足可追究性是不够的,它还应遵循公平性原则.可追究性仅要求在协议完成后,各个主体拥有充分的证据.而对于协议异常中止时,各个主体的状态未加考虑.公平性原则要求在协议异常中止时,各个主体地位相同,没有任何主体处于有利地位.

在此节中,我们将分析 IBS 协议(internet billing service protocol)来说明缺乏公平性所产生的漏洞.IBS 协议[3]是由卡内基-梅隆大学开发的电子商务协议,该协议分为如下 3 个部分.

确定价格

(1) $E\rightarrow S$: $\{\text{Price Request}\}_{K_e^{-1}}$

(2) $S\rightarrow E$: $\{\text{Price}\}_{K_s^{-1}}$

在确定价格的过程中,用户 E 首先向服务提供方 S 发送一个用它的私有密钥 K_e^{-1} 签名的价格咨询消息.如果服务提供方 S 同意这个价格,他就发送一个用他的私有密钥 K_s^{-1} 签名的价格同意消息.

提供服务

(3) $E\rightarrow S$: $\{\{\text{Price}\}_{K_s^{-1}}\text{Price}\}_{K_e^{-1}}$

(4) $S\rightarrow$Invoice: $\{\{\text{Price}\}_{K_e^{-1}}\text{Price}\}_{K_e^{-1}}$

(5) $S\rightarrow E$: $\{\text{Service}\}_{K_e^{-1}}$

(6) $E\rightarrow S$: $\{\text{Service Acknowledge}\}_{K_e^{-1}}$

(7) $S\rightarrow$Invoice: $\{\{\text{Service Acknowledge}\}_{K_e^{-1}}\}_{K_s^{-1}}$

在提供服务协议中,第 1 条消息用户 E 向服务提供方 S 发送一个服务请求,服务提供方 S 把这条消息复制到发票上,并发送一条签名的服务消息给用户 E.用户 E 收到服务后,发送一个签名的服务认可消息给服务提供方 S,服务提供方 S 把它复制到发票上.

传递发票

(8) $E\rightarrow S$: $\{\text{Invoice Request}\}_{K_e^{-1}}$

(9) $S\rightarrow B$: $\{\{\text{Invoice}\}_{K_b}\}_{K_s^{-1}}$

(10) $B\rightarrow S$: $\{\{\text{Invoice}\}_{K_s}\}_{K_b^{-1}}$

(11) $B\rightarrow E$: $\{\{\text{Invoice}\}_{K_e}\}_{K_b^{-1}}$

在传递发票协议中,用户 E 给服务提供方 S 发送一个发票请求.服务提供方 S 向银行机构 B 发送一张先用银行机构的公开密钥加密,然后用他的私有密钥签名的发票.银行验证发票后,进行相应的转帐处理,将发票用他们的公开密钥加密后再用银行机构的私有密钥签名,然后分别发送给用户和服务提供方.

利用 Kailar 逻辑可以证明,IBS 协议在确定价格和提供服务两个阶段满足可追究性原则[2].但是,IBS 协议不满足公平性原则.

在 IBS 协议中,服务提供方 S 在第(5)步为用户 E 提供服务.按协议的设计,用户 E 收到服务后在第(6)步提供给服务提供方一个签名的确认消息.但如果用户 E 是不诚实的,他可以在收到服务后不提供确认消息,协议至此中止.此时,服务提供方就无法提供他向用户 E 提供服务的证据.而用户 E 已获得了服务,他处于有利地位.

2.2 CMP1 协议和 CMP2 协议

与信念逻辑相似,Kailar 逻辑必须对参与协议的各个主体进行初始化假设.但在 Kailar 逻辑中,这一过程是

非形式化的,因而极易出错.下面,我们将通过对 CMP1 协议的分析说明非形式化的初始化假设极易出错,从而导致协议分析的失败.

CMP1 和 CMP2 协议是 Robert Deng 和 Li Gong 等人提出的认证电子邮件协议[4](certified electronic mail).这些协议为电子邮件的传输提供非否认服务.CMP1 和 CMP2 协议的区别在于,CMP1 协议没有提供 E-mail 内容的加密保护.下面,我们将通过对 CMP1 的分析,指出 Kailar 逻辑在解释过程中由于非形式化而产生的缺陷.

首先介绍 CMP1 协议.

(1) $A\rightarrow B:h(m),\{k\}_{K_{TTP}},\{\{m\}_{K_a^{-1}}\}_k$

(2) $B\rightarrow A:\{h(m)\}_{K_b^{-1}},\{k\}_{K_{TTP}},\{\{m\}_{K_a^{-1}}\}_k$

(3) $TTP\rightarrow B:\{\{m\}_{K_a^{-1}}\}_{K_{TTP}^{-1}}$

(4) $TTP\rightarrow A:\{\{h(m)\}_{K_b^{-1}},(B,m)\}_{K_{TTP}^{-1}}$

其中 k 是 A 与 TTP 共享的会话密钥.

第(1)步 A 选择一个会话密钥 k,然后把消息 m 的摘要 $h(m)$、消息 m 签名后用 k 加密的密文 $\{\{m\}_{K_a^{-1}}\}_k$ 和加密的会话密钥 $\{k\}_{K_{TTP}}$ 发送给 B.第(2)步,B 对 $h(m)$ 签名,并连同后两部分转发给 TTP.TTP 收到后,通过解密获取 $\{m\}_{K_a^{-1}}$,然后在第(3)步将它用自己的私有密钥签名后传送给 B;在第(4)步将 B 签过名的摘要和 (B,m) 用自己的私有密钥签名后传送给 A.

协议分析过程如下.

协议的目的是为电子邮件传输提供非否认服务,协议设计者希望达到下面的目标:

$$A \text{ CanProve } (B \text{ Recieved } m), \tag{G_1}$$

$$B \text{ CanProve } (A \text{ Sent } m). \tag{G_2}$$

首先,对协议语句理解如下:

(2.1) TTP Receives $h(m)$ SignedWith K_b^{-1},

(2.2) TTP Receives m SignedWith K_a^{-1},

(3) B Receives (m SignedWith K_a^{-1}) SignedWith K_{TTP}^{-1},

(4) A Receives ($h(m)$) SignedWith K_b^{-1},(B,m)) SignedWith K_{TTP}^{-1}.

列举初始化假设如下:

A1　A,B CanProve (K_{TTP} Authenticates TTP),

A2　A,TTP CanProve (K_b Authenticates B),

A3　B,TTP CanProve (K_a Authenticates A),

A4　A,B CanProve (TTP IsTrustedOn (TTP Says)),

A5　(A Says m)⇒(A sent m),

A6　(B Says $h(m)$)→(B received $h(m)$),

A7　(TTP Says (B,m))⇒(TTP Says m 成功发送给 B),

A8　(B Received $h(m)$) ∧ (m 成功发送给 B)⇒(B received m).

推理过程如下:

由消息(3)和假设 A1,应用签名规则,

$$B \text{ CanProve } (TTP \text{ Says } (m \text{ SignedWith } K_a^{-1})).$$

根据假设 A4,B 信任 TTP,用信任规则,

$$B \text{ CanProve } (m \text{ SignedWith } K_a^{-1}).$$

再用一次签名规则,

$$B \text{ CanProve } (A \text{ Says } m).$$

由上述公式,用假设 A5 和推理规则,有

$$B \text{ CanProve } (A \text{ Sent } m). \tag{G_2}$$

消息(4)等价于

(4.1) A Receives ($h(m)$) SignedWith K_b^{-1}) SignedWith K_{TTP}^{-1},

(4.2) A Receives (B,m) SignedWith K_{TTP}^{-1}.

由(4.1)和假设 A1,应用签名规则,

$$A \text{ CanProve } (TTP \text{ Says } (h(m) \text{ SignedWith } K_b^{-1})).$$

再由假设 A4 和信任规则,

$$A \text{ CanProve } (h(m) \text{ SignedWith } K_b^{-1}).$$

由假设 A2,再用一次签名规则,

$$A \text{ CanProve } (B \text{ Says } h(m)).$$

由假设 A6,用推理规则,

$$A \text{ CanProve } (B \text{ Receives } h(m)). \qquad (*)$$

由(4.2)和假设 A1,应用签名规则,

$$A \text{ CanProve } (TTP \text{ Says } (B,m)).$$

运用假设 A7 和推理规则,

$$A \text{ CanProve } (m \text{ 成功发送给 } B). \qquad (**)$$

由公式(*)和(**),应用连接规则,

$$A \text{ CanProve } ((B \text{ Receives } h(m)) \wedge (m \text{ 成功发送给 } B)).$$

由上面的结果,应用假设 A8 和推理规则,

$$A \text{ CanProve } (B \text{ Received } m). \qquad (G_1)$$

这就证明了协议满足可追究性,符合协议设计者的目标.

在证明过程中引入了 8 条初始化假设 A1～A8,其中 A1～A4 是基本的,它们是协议设计者假定的协议运行的前提条件. A5～A8 是协议证明者为了证明协议的可追究性而作的假设. 其中 A5,A6,A7 是对一些推导的中间结果的解释. A8 实质上是协议证明者作出的一个推理,他认为,如果能证明 B 收到了 $h(m)$以及 m 已经送达 B,那么就能证明 B Received m.

在用 Kailar 逻辑进行形式化分析的过程中,无法用形式化的方法确定协议证明之前需要添加哪些假设. 许多假设都是协议证明者在推导时加入的,例如本例中的 A5～A8. 不幸的是,不恰当地引入这些假设会导致协议分析的失败.

例如,对本协议稍作修改,称为 CMP1(b):

(1) $A \rightarrow B$: $h(m)$,$\{k\}_{K_{TTP}}$,$\{\{m\}_{K_a^{-1}}\}_k$,

(2.1) $B \rightarrow A$: $\{h(m)\}_{K_b^{-1}}$,

(2.2) $B \rightarrow TTP$: $\{k\}_{K_{TTP}}$,$\{\{m\}_{K_a^{-1}}\}_k$,

(3) $TTP \rightarrow B$: $\{\{m\}_{K_a^{-1}}\}_{K_{TTP}^{-1}}$,

(4) $TTP \rightarrow A$: $\{(B,m)\}_{K_{TTP}^{-1}}$.

协议可理解为:

(2.1) A Receives ($h(m)$ SignedWith K_b^{-1}),

(2.2) TTP Receives (m SignedWith K_a^{-1}),

(3) B Receives (m SignedWith K_a^{-1}) SignedWith K_{TTP}^{-1},

(4) A Receives (B,m) SignedWith K_{TTP}^{-1}.

初始化假设仍采用协议 CMP1 的 A1～A8,推理过程如下:

由消息(3),同前可证

$$B \text{ CanProve } (A \text{ Sent } m). \qquad (G_2)$$

由消息(2.1)和假设 A2,应用签名规则,

$$A \text{ CanProve } (B \text{ Says } h(m)).$$

由假设 A6,用推理规则,

$$A \text{ CanProve } (B \text{ Receives } h(m)). \qquad (*)$$

由消息(4),同前可证,

$$A \text{ CanProve } (m \text{ 成功发送给 } B). \qquad (**)$$

利用结果(*)和(**)以及假设 A8,同前可证,

$$A \text{ CanProve } (B \text{ Received } m). \qquad (G_1)$$

至此,我们已利用 Kailar 逻辑证明了协议 CMP1(b)的可追究性.事实上,协议 CMP1(b)是不可追究的.假定通信双方 A 是诚实的,而 B 是不诚实的.在协议的(2.1)步,B 发送给 A 的是$\{h(m')\}_{K_b^{-1}}$,m'是不同于 m 的另外一个消息.那么当协议执行完后,A 得到的是$\{h(m)'\}_{K_b^{-1}}$和$\{(B,m)\}_{K_{TTP}^{-1}}$,他不能拿出足够的证据来证明 B 收到的是 m 而不是 m'.而产生这一错误分析结果的原因在于初始化假设 A8.初始化假设 A8 在 CMP1 中成立是基于以下事实:TTP 在收到$\{h(m)'\}_{K_b^{-1}}$,$\{k\}_{K_{TTP}}$,$\{\{m\}_{K_a^{-1}}\}_k$ 之后,检查了 $h(m')$与 m 的一致性.由于 B 收到了 $h(m')$与相应的 m,A 可以证明 B 收到了 m.而在 CMP1(b)中,由于 B 在(2.1)步中已先将$\{h(m)'\}_{K_b^{-1}}$发送给 A,TTP 无法验证 $h(m')$与 m 的一致性,A 只能证明 B 收到了 $h(m')$,而无法证明 B 收到了 m.

2.3 非否认协议(Zhou-Gollman)

在 Kailar 逻辑中,公式 A CanProve x 要求主体 A 向 B 证明公式 x 时不泄漏任何秘密 $y(y\neq x)$给 B,这就使得 Kailar 逻辑无法分析那些签名的密文,从而限制了其使用的范围.

实际上,由于保密的要求,一些协议的消息经过加密后才能传输.同时,由于这些消息的信息量较大,故通常采用单钥加密算法进行加密.按照 Kailar 逻辑的语义,参与协议的主体不能公开加密密钥,从而无法证明这些消息的来源.

下面,我们采用 J. Zhou 和 D. Gollman 设计的签订电子合同的协议来说明 Kailar 逻辑的这一局限.在这个协议中,J. Zhou 和 D. Gollman 提出了一种基于 ftp 的方法[5],并用 $A\leftrightarrow TTP:m$ 表示主体 A 通过多次 ftp 操作,从 TTP 处获得了消息 m.

现在,我们介绍 J. Zhou 和 D. Gollman 设计的协议[6].

(1) $A\rightarrow B$: $\{M\}_K$,$\{\{M\}_K\}_{K_a^{-1}}$

(2) $B\rightarrow A$: $\{\{M\}_K\}_{K_b^{-1}}$

(3) $A\rightarrow TTP$: $\{K,\{K\}_{K_a^{-1}}\}_{K_{a,TTP}}$

(4) $B\leftrightarrow TTP$: K,$\{K\}_{K_{TTP}^{-1}}$

(5) $A\leftrightarrow TTP$: $\{K\}_{K_{TTP}^{-1}}$

其中 $K_{a,ttp}$是 A 与 TTP 共享的密钥.

在第(1)、(2)步,A 选择一个密钥 K 对 M 进行加密,然后连同他对$\{M\}_k$ 的签名发送给 B.B 对$\{M\}_k$签名后返回给 A.第(3)步,A 把密钥 K 连同他对 K 的签名用他与 TTP 的共享密钥加密后发送给 TTP.第(4)、(5)步,B 通过 ftp 操作从 TTP 获取 K 和 TTP 对 K 的签名.A 通过 ftp 操作从 TTP 获得 TTP 对 K 的签名.

协议分析过程如下.

协议的目标为:

$$A \text{ CanProve } (B \text{ Says } M). \qquad (G_1)$$

$$B \text{ CanProve } (A \text{ Says } M). \qquad (G_2)$$

对协议的理解如下:

(1) B Revieves (Encrypted M) SignedWith K_a^{-1},

(2) A Revieves (Encrypted M) SignedWith K_b^{-1},

(3) TTP Recieves K SignedWith K_a^{-1},

(4) B Revieves K SignedWith K_{TTP}^{-1},

(5) A Revieves K SignedWith K_{TTP}^{-1}.

列举初始化假设如下:

A1 A,B CanProve (K_{TTP} Authenticates TTP),

A2 A,TTP CanProve (K_b Authenticates B),

A3 B,TTP CanProve (K_a Authenticates A),

A4 A,B CanProve (TTP IsTrustedOn (TTP Says)).

由(1)和A3,应用签名规则,

$$B \text{ CanProve } (A \text{ Says } (\text{Encrypted } M)).$$

由(4)和A1,应用签名规则,

$$B \text{ CanProve } (TTP \text{ Says } K).$$

由A4,应用信任规则,

$$B \text{ CanProve } (K).$$

对上面结果应用连接规则,

$$B \text{ CanProve } ((A \text{ Says } (\text{Encrypted } M)) \wedge (K)).$$

由于B无法泄露K给公众来证明A应对明文M的可追究性负责.在这种情况下,Kailar建议改变加密和签名的先后顺序,即将协议中形如$\{\{m\}_K\}_{K_a^{-1}}$的报文改变为形如$\{\{m\}_{K_a^{-1}}\}_K$的报文,从而得到签名的明文,以便作形式化分析.但通过观察上述协议,我们可以发现,即使在第(1)步中,A将$\{\{m\}_K\}_{K_a^{-1}}$改为$\{\{m\}_{K_a^{-1}}\}_K$,B仍然无法生成报文$\{\{m\}_{K_b^{-1}}\}_K$,除非加密运算和签名是可交换的.因此,A不可能得到签名$\{m\}_{K_b^{-1}}$来证实B收到了报文m.

另一方面,该协议的会话密钥K是临时生成的,仅用于当前协议报文的加密,因而在仲裁时可出示密钥K.

3 结 论

根据前面3个例子的分析,我们认为Kailar逻辑存在3个缺陷:

(1) 逻辑只能分析协议的可追究性,不能分析协议的公平性.这是它最主要的缺陷.

(2) 逻辑在解释协议语句时,只能解释那些签过名的明文消息,这就限制了它的使用范围.因此,Kailar逻辑需要作进一步的扩充,使它能解释和分析签过名的加密消息.

(3) Kailar逻辑在推理之前需要引入一些初始化假设.不幸的是,引入这些初始化假设是一个非形式化的过程,不当地引入初始化假设会导致协议分析的失败.所以,如何形式化地列举初始化假设和解释协议语句是需要解决的问题.

致谢 本文的研究工作得到国家自然科学基金资助,此项目编号为69673016.在此表示感谢!

参考文献

1 Abadi M, Burrows M, Needham M. A logic of authentication. ACM Transactions on Computer Systems, 1990, 8(1): 18~36

2 Kailar R. Accountability in electronic commerce protocols. IEEE Transactions on Software Engineering, 1996, 22(5): 313~328

3 O'Toole K R. The Internet billing server transaction protocol alternatives. INI TR 1994—1, Carnegie Mellon University: Information Networking Institute. 1994

4 Deng R H, Gong L. Practical protocols for certified electronic mail. Journal of Network and Systems Management, 1996, 4(3): 279~297

5 Postel J, Reynolds J. File transfer protocol. RFC 959, 1985

6 Zhou J, Gollman D. A fair non-repudiation protocol. In: Roscheisen M, Serban C eds. Proceeding of 1996 IEEE Symposium on Security and Privacy. Oakland, CA: IEEE Computer Society Press, 1996. 55~61

Limitations of Kailar Logic

ZHOU Dian-cui　QING Si-han　ZHOU Zhan-fei

(*Institute of Software　The Chinese Academy of Sciences　Beijing*　100080)

(*Engineering Research Center for Information Security Technology　The Chinese Academy of Sciences　Beijing*　100080)

Abstract　There is a growing interest in the design and development of electronic commerce protocols. Accountability is the ability to hold individuals or organizations accountable for transactions. Without such assurances, electronic transactions can be susceptible to disputes. Rajashekar Kailar has proposed a framework for the analysis of communication protocols which require accountability. The authors call this framework Kailar logic. In this paper, the authors find this framework has three limitations. Firstly, the framework cannot analyze fairness of protocols. Secondly, articulating initial state assumptions is an informal and error-prone step. At last, the messages with encrypted contents in the protocol cannot be interpreted.

Key words　Accountability, electronic commerce, protocol, protocol analysis.