文章编号:1001 - 9081(2008)08 - 1928 - 03

一种挂号电子邮件协议的设计及其形式化分析

高悦翔[1,2],彭代渊[1]
(1. 西南交通大学 信息科学与技术学院,成都 610031; 2. 四川师范大学 计算机科学学院,成都 610068)
(gyx415@163.com)

摘 要:挂号电子邮件协议需要具备保密性、不可否认性及公平性。提出了一种基于在线第三方的挂号电子邮件协议,以满足挂号电子邮件的一般安全特性。利用扩展 Kailar 逻辑对该协议进行分析,说明该协议满足不可否认性及公平性,并具有抗篡改、重放等攻击及第三方无法获得邮件内容等优点。

关键词:挂号电子邮件协议;不可否认性;公平性;形式化分析;Kailar 逻辑
中图分类号: TP309 **文献标志码**:A

Design and formal analysis of certified E-mail protocol

GAO Yue-xiang[1,2], PENG Dai-yuan[1]
(1. *School of Information Science and Technology, Southwest Jiaotong University, Chengdu Sichuan* 610031, *China*;
2. *School of Computer Science, Sichuan Normal University, Chengdu Sichuan* 610068, *China*)

Abstract: There are some goals of Certified E-mail Protocol: confidentiality, non-repudiation and fairness. This paper proposes a Certified E-mail Protocol based on the online third party to satisfy the secure properties. The protocol analyzed by extended Kailar logic can achieve the non-repudiation, fairness as well as the other advantages that it can resist the attacks as distort, replay and the third party can't read the E-mail.

Key words: certified E-mail protocol; non-repudiation; fairness; formal analysis; Kailar logic

0 引言

随着电子商务、电子政务的迅速开展,对挂号电子邮件的需求日益增加。挂号电子邮件协议在具有保密性的同时还应具有不可否认性及公平性,即电子邮件客户事后能够确认和追究收信或者发信的责任,同时收发双方要么都得到了他们期望得到的内容,要么都没有得到。针对这一状况,国内外学者对挂号电子邮件开展了大量研究。文献[1,2,3]分别提出了第三方在线的挂号电子邮件协议,其中文献[1]中的协议不满足公平性,且需要时钟同步问题。文献[2]中的协议无法做到不可否认。文献[3]中的协议存在第三方可以获得通信双方传递的消息的缺点且不具有公平性。文献[4,5]别介绍了离线第三方的挂号电子邮件协议,执行这类协议时,第三方在正常情况下不参与协议,当通信双方出现争议时才参与协议以解决纠纷。文献[4]中的协议不满足可追究性的要求,文献[5]中的协议不满足公平性。

文献[6]中提出了基于在线第三方的挂号电子邮件协议,该协议希望通过三个步骤的邮件传输协议,以满足不可否认性及公平性,同时第三方无法获得邮件的内容。遗憾的是该协议会导致发送方无法收到收方不可否认证据从而使协议不满足不可否认性。本文首先分析了文献[6]提出的协议存在的缺陷,并在此基础上提出了一个基于在线第三方的挂号电子邮件协议,最后对本文提出的协议进行了形式化证明。

1 文献[6]中协议的分析

文献[6]提出了一个第三方在线的挂号电子邮件协议,该协议的设计目标是能抵御常见的篡改和重放攻击,并减少对可信第三方的信赖程度,保证邮件的机密性,除了邮件预期的接收者能读取其中的内容,其他的任何主体包括可信第三方都不能读取邮件内容。

1.1 协议步骤

1) M1: $S \rightarrow R$: $L, S, \{M\}_K, \{\{K\}_{K_R}\}_{K_{TTP}}, \{L, H(\{M\}_K), H(\{\{K\}_{K_R}\}_{K_{TTP}})\}_{K_S^{-1}}$

2) M2: $R \rightarrow TTP$: $L, S, R, \{\{K\}_{K_R}\}_{K_{TTP}}, \{L, H(\{M\}_K), H(\{\{K\}_{K_R}\}_{K_{TTP}})\}_{K_S^{-1}}, \{L, H(\{M\}_K)\}_{K_R^{-1}}$

3) M3: $T \rightarrow R$: $L, \{K\}_{K_R}$

该协议包括三个步骤,协议中包括三方:发送者 S、接收者 R、可信第三方 TTP。M 是主体 S 发送给主体 R 的消息,用 $S \rightarrow R: x$ 表示主体 S 向 R 发送数据 x。S 具有公钥 K_S 及私钥 K_S^{-1}, R 具有公钥 K_R 及私钥 K_R^{-1}, TTP 具有公钥 K_{TTP} 及私钥 K_{TTP}^{-1}, K 是 S 随机生成的 S 和 R 之间的会话密钥。$\{x,y\}$ 表示 x 和 y 按此顺序的串接。$H(M)$ 表示对 x 使用散列函数得到的值, $\{M\}_K$ 表示使用密钥 K 对 M 进行加密运算得到的密文, $\{M\}_{K_S^{-1}}$ 表示 S 用私钥对 M 的签名。其他符号及流程说明参见文献[6]。

1.2 文献[6]协议的安全隐患

文献[6]中提出的协议可以保证邮件的保密性,但其协议只有三个步骤,无法满足挂号电子邮件的不可否认性及公平性的要求,协议缺陷分析如下:

1) 文献[6]协议中收方的不可否认证据需要消息 M4,即 $(L, \{L, H(\{M\}_K)\}_{K_R^{-1}}, \{L, H\{(K)\}_{K_R^{-1}})$。而消息 M4 在原协议步骤中不存在,故 S 无法获得 M4,也就无法获得收方的不可否认证据,亦即对于发送方而言不满足不可否认性。

收稿日期:2008 - 02 - 20;**修回日期**:2008 - 04 - 10。

作者简介:高悦翔(1975 -),男,四川成都人,讲师,博士研究生,主要研究方向:信息安全; 彭代渊(1955 -),男,四川资阳人,教授,博士生导师,主要研究方向:密码学、信息安全、编码理论及扩频序列。

2) 消息 M4 中的两个部分都是由 R 签名得到,故该消息只有 R 可以构造。R 完全可以在收到消息 M3 后不发送 $M4$ 给 S,这样 S 也无法获得收方的不可否认证据,使得协议不能满足不可否认性,故在该协议中对 M4 的设计存在安全隐患。

3) 该协议第三步 R 收到的消息 M3 没有 TTP 的签名,故 R 无法确认消息是否来自 TTP。攻击者可以利用这一点,在协议的第三步冒充 TTP 发送错误的 $\{K\}_{K_R}$ 给 R,使得 R 无法阅读 M 的内容,这对于 R 来说是不公平的。

2　一个新的挂号电子邮件协议

在分析文献[6]缺陷的基础上,本文提出了一个新的基于在线可信第三方的挂号电子邮件协议。本文中的符号沿用文献[6]中的符号,协议步骤如下:

1) M1: $S \rightarrow R$:$L,S,\{M\}_K,\{\{K\}_{K_R}\}_{K_{TTP}},\{L,H(\{M\}_K),H(\{\{K\}_{K_R}\}_{K_{TTP}})\}_{K_S^{-1}}$

2) M2: $R \rightarrow TTP$:$L,S,R,\{\{K\}_{K_R}\}_{K_{TTP}},\{L,H(\{M\}_K),H(\{\{K\}_{K_R}\}_{K_{TTP}})\}_{K_S^{-1}},\{L,H(\{M\}_K),\{\{K\}_{K_R}\}_{K_{TTP}}\}_{K_R^{-1}}$

3) M3: $T \rightarrow R$:$L,\{\{K\}_{K_R}\}_{K_{TTP}^{-1}}$

4) M4: $T \rightarrow S$:$L,\{L,H(\{M\}_K),\{\{K\}_{K_R}\}_{K_{TTP}}\}_{K_R^{-1}},\{L,R,H(\{M\}_K),\{K\}_{K_R}\}_{K_{TTP}^{-1}}$

其中第 3) 步和第 4) 步由 TTP 同时向 S 和 R 发出。

协议说明:

1) K 是 S 随机生成的会话密钥,L 用于唯一标识一次会话,可以是随机值也可以是一个时间戳,以确保每一条消息不会被重放攻击。

2) R 在确认 $\{M\}_K$ 与 $H(\{M\}_K)$,$\{\{K\}_{K_R}\}_{K_{TTP}}$ 与 $H(\{\{K\}_{K_R}\}_{K_{TTP}})$ 匹配后,向 TTP 发送消息 M2,否则放弃本次协议。若上述匹配不满足,R 不会发送 M2 给 TTP,协议也就无法完成 3) 及 4),即若 S 存在欺骗的可能,他将无法得到 R 的不可否认证据。若 R 放弃,由于 R 未获得 K,故 R 无法获得 M,因此 R 的放弃没有破坏 S 的不可否认性及公平性。

3) TTP 在确认 $\{\{K\}_{K_R}\}_{K_{TTP}}$ 与 $H(\{\{K\}_{K_R}\}_{K_{TTP}})$ 以及 S 拥有的 $H(\{M\}_K)$ 与 R 发送的 $H(\{M\}_K)$ 匹配的情况下,分别发送 $M3$ 与 $M4$ 给 R 和 S。这样,一方面保证 TTP 能够判断 R 是否发送了伪造的 $H(\{M\}_K)$ 来欺骗 TTP。另一方面由 TTP 发送收方不可否认证据给 S,防止了 S 收不到收方不可否认证据的情况。

4) 整个过程中邮件 M 被加密为 $\{M\}_K$,TTP 不能获得密钥 K。同时邮件的加密密钥 K 被 S 用 R 的加密密钥 K_R 加密,从而保证了除了邮件预期的接收者能读取其中的内容,其他的任何主体包括可信第三方都不能读取邮件内容。

3　新协议的形式化证明

认证协议的设计常因一些细微的问题产生安全缺陷,为此有必要对本文的协议进行形式化证明。Kailar 提出了一种安全协议的逻辑分析方法[7],扩展了信念逻辑的分析范围,可以用于分析电子商务协议的可追究性。文献[8]针对 Kailar 逻辑存在的缺陷进行了扩展,本文利用文献[8]中提出的形式化方法对本文提出的协议进行形式化分析。

3.1　扩展 Kailar 逻辑的推理规则

扩展 Kailar 逻辑的逻辑构件参见文献[8]。该逻辑由 1 个推理规则和 8 个公理组成。

1) 推理规则:$(\vdash \varphi) \wedge (\vdash(\varphi \Rightarrow \psi)) \Rightarrow \vdash \psi$。

上述推理规则说明,由 $\vdash \varphi$ 和 $\vdash(\varphi \Rightarrow \psi)$ 可以得到 $\vdash \psi$。

2) 8 个公理:

A1 连接公理:A CanProve $x \wedge A$ CanProve $y \Rightarrow A$ CanProve $(x \wedge y)$。

A2 蕴涵公理:A CanProve $x \wedge (x \Rightarrow y) \Rightarrow A$ CanProve y。

A3 签名公理:$(A\ Has \{m\}_{K^{-1}}) \wedge A$ CanProve $PK(B,K) \Rightarrow A$ CanProve (B Claims m)。

A4 管辖公理:A CanProve(B Controls x) $\wedge A$ CanProve(B Claims x) $\Rightarrow A$ CanProve x。

A5 密文理解公理:

A CanProve (B Claims $\{m\}_K$) $\wedge A$ CanProve (B Claims K) $\Rightarrow A$ CanProve (B Claims m)。

A6 拥有公理:A Received $m \vee A$ Fetched $m \vee A$ Generated $m \Rightarrow A$ Has m。

A7 接收公理:A Received $\{m\}_K \wedge A$ Has $\bar{K} \Rightarrow A$ Received m。

A8 取到公理:A Fetched $\{m\}_K \wedge A$ Has $\bar{K} \Rightarrow A$ Fetched m。

针对 Kailar 逻辑对密文消息分析不足的状况,本文在文献[8]的基础上增加一条公理:

A9 A CanProve (B Claims $\{x\}_{K_A}$) $\wedge A$ Has $K_A^{-1} \Rightarrow A$ CanProve B Claims x,即若 A 能证明 B 对 $\{x\}_{K_A}$ 负责,而 A 又拥有 K_A^{-1},于是 A 可证明 B 对 x 负责。

3.2　对本文协议的分析

1) 协议分析的准备

① 列出初始拥有集合:$O_S^0 = \{K_S^{-1},K_S,K_R,K_{TTP},K\}$,$O_R^0 = \{K_R^{-1},K_S,K_R,K_{TTP}\}$

② 初始假设集合

i) 基本假设

B1 S CanProve $PK(R,K_R)$,B2 R CanProve $PK(S,K_S)$,B3 S,R CanProve $PK(TTP,K_{TTP})$

ii) 可信假设

T1 S,TTP,R CanProve R Controls $match(\{M\}_K,H(\{M\}_K))$

T2 TTP Claims $\{K\}_{K_R} \Rightarrow TTP$ Claims $match(\{\{K\}_{K_R}\}_{K_{TTP}},H(\{\{K\}_{K_R}\}_{K_{TTP}}))$

T3 TTP Claims(将 $\{K\}_{K_R}$ 发送给 R) $\Rightarrow TTP$ Claims $match(M',M'')$

为方便起见,此处 $M' = \{L,H(\{M\}_K),H(\{\{K\}_K\}_{K_{TTP}})\}_{K_S^{-1}}$,$M'' = \{L,H(\{M\}_K),\{\{K\}_{K_R}\}_{K_{TTP}}\}_{K_R^{-1}}$,以下 M' 及 M'' 与此处相同。

T4 TTP Claims $match(M',M'') \Rightarrow TTP$ Received M''

T5 TTP Claims $H(\{M\}_K) \Rightarrow TTP$ Received M''

T6 R Claims $match(\{M\}_K,H(\{M\}_K)) \Rightarrow R$ Has $\{M\}_K$

T7 S CanProve TTP Claims $\{K\}_{K_R} \Rightarrow S$ CanProve TTP Claims (将 $\{K\}_{K_R}$ 发送给 R)

iii) 协议理解假设

C1 TTP Received $M'' \Rightarrow R$ Claims $match(\{M\}_K,H(\{M\}_K))$

C2 TTP Claims $match(\{\{K\}_{K_R}\}_{K_{TTP}},H(\{\{K\}_{K_R}\}_{K_{TTP}})) \Rightarrow S$ Claims $\{K\}_{K_R}$

C3 S Claims $H(\{M\}_K) \wedge S$ Has $\{M\}_K \wedge match(\{M\}_K,$

$H(\{M\}_K))\Rightarrow S$ Claims $\{M\}_K$

C4 R Claims $match(\{M\}_K,H(\{M\}_K))\Rightarrow S$ Generated $\{M\}_K$

C5 R Claims $\{\{K\}_{K_R}\}_{K_{TTP}}\wedge TTP$ Claims (将$\{K\}_{K_R}$发送给$R)\Rightarrow R$ Claims $\{K\}_{K_R}$

③ 列举 *EOO* 和 *EOR*

$EOO=\{L,H(\{M\}_K),H(\{\{K\}_{K_R}\}K_{TTP})\}_{K_S^{-1}},\{\{K\}_{K_R}\}_{K_{TTP}^{-1}}$

$EOR=\{L,H(\{M\}_K),\{\{K\}_{K_R}\}_{K_{TTP}}\}_{K_R^{-1}},\{L,R,H(\{M\}_K),\{K\}_{K_R}\}_{K_{TTP}^{-1}}$

2) 可追究性分析

① 列举可追究目标：R CanProve (S Claims M), S CanProve (R Claims M)

② 分析 *EOO* 与 *EOR* 的设计是否符合可追究性要求

假定$EOO\in O_R$,即$\{L,H(\{M\}_K),H(\{\{K\}_{K_R}\}K_{TTP})\}_{K_S^{-1}}\in O_R$且$\{\{K\}_{K_R}\}_{K_{TTP}^{-1}}\in O_R$。

故：

R Has$\{L,H(\{M\}_K),H(\{\{K\}_{K_R}\}K_{TTP})\}_{K_S^{-1}}$ (1)

R Has$\{\{K\}_{K_R}\}_{K_{TTP}^{-1}}$ (2)

由 A3,B2 及式(1) 可得：

R CanProve S Claims $H(\{M\}_K)$ (3)

由 A3,B3 及式(2) 可得 R CanProve *TTP* Claims $\{K\}_{K_R}$。

由上式及 A2,C2 可得 R CanProve *TTP* Claims (将$\{K\}_{K_R}$发送给R)。

由上式及 A2,T3 可得 R CanProve *TTP* Claims $match(\{\{K\}_{K_R}\}_{K_{TTP}},H(\{\{K\}_{K_R}\}_{K_{TTP}}))$。

由上式及 A2,T4 可得 R CanProve *TTP* Received M''。

由上式及 A2,C1 可得：

R CanProve R Claims $match(\{M\}_K,H(\{M\}_K))$ (4)

由上式及 A4,T1 可得：

R CanProve $match(\{M\}_K,H(\{M\}_K))$ (5)

由式(4) 及 A2,C4 可得：

R CanProve S Generated $\{M\}_K$ (6)

由式(6) 及 A2,A6 可得：

R CanProve S Has$\{M\}_K$ (7)

由式(3),(5),(7) 及 A1 可得

R CanProve (S Claims $H(\{M\}_K)\wedge S$ Has$\{M\}_K\wedge match(\{M\}_K,H(\{M\}_K))$)。

由上式及 C3 可得：

R CanProve S Claims $\{M\}_K$ (8)

由式(2) 及 A3,B3 可得 R CanProve *TTP* Claim $\{K\}_{K_R}$。

由上式及 A2,T2 可得 R CanProve *TTP* Claims $match(\{\{K\}_{K_R}\}_{K_{TTP}},H(\{\{K\}_{K_R}\}_{K_{TTP}}))$。

由上式及 A2,C2 可得 R CanProve S Claims $\{K\}_{K_R}$。

由上式及 A2,A9 可得 R CanProve S Claims K。

由上式、式(8) 及 A5 可得：

R CanProve S Claims M (9)

假定 $EOR\in O_S$, 即 $\{L,H(\{M\}_K),\{\{K\}_{K_R}\}_{K_{TTP}}\}_{K_R^{-1}}\in O_S$、$\{L,R,H(\{M\}_K),\{K\}_{K_R}\}_{K_{TTP}^{-1}}\in O_S$, 亦即 S Has$\{L,H(\{M\}_K),\{\{K\}_{K_R}\}_{K_{TTP}}\}_{K_R^{-1}}$ 且 S Has$\{L,R,H(\{M\}_K),\{K\}_{K_R}\}_{K_{TTP}^{-1}}$。

由 S Has$\{L,R,H(\{M\}_K),\{K\}_{K_R}\}_{K_{TTP}^{-1}}$及 A2、B3 可得 S CanProve *TTP* Claim $H(\{M\}_K)$。

由上式及 A2、T5 可得 S CanProve *TTP* Received M''。

由上式及 A2、C1 可得：

S CanProve R Claims $match(\{M\}_K,H(\{M\}_K))$ (10)

由上式及 A2、T6 可得：

S CanProve R Has$\{M\}_K$ (11)

由式(10) 及 A4、T1 可得：

S CanProve $match(\{M\}_K,H(\{M\}_K))$ (12)

由 S Has$\{L,H(\{M\}_K),\{\{K\}_{K_R}\}_{K_{TTP}}\}_{K_R^{-1}}$及 A2、B1 可得：

S CanProve R Claim $H(\{M\}_K)$ (13)

由式(11)、(12)、(13)、A1 可得：

S CanProve (R Claims $H(\{M\}_K)\wedge R$ Has$\{M\}_K\wedge match(\{M\}_K,H(\{M\}_K))$)

由上式及 A2、C3 可得：

S CanProve R Claims $\{M\}_K$ (14)

由 S Has $\{L,R,H(\{M\}_K),\{K\}_{K_R}\}_{K_{TTP}^{-1}}$及 A2、B3 可得 S CanProve *TTP* Claim $\{K\}_{K_R}$。

由 S Has $\{L,H(\{M\}_K),\{\{K\}_{K_R}\}_{K_{TTP}}\}_{K_R^{-1}}$及 A2、B3 可得：

S CanProve R Claim $\{\{K\}_{K_R}\}_{TTP}$ (15)

由 S CanProve *TTP* Claim $\{K\}_{K_R}$, A2、T7 可得：

S CanProve *TTP* Claims (将$\{K\}_{K_R}$发送给R) (16)

由式(15)、(16) 及 A2、C5 可得 S CanProve R Claim $\{K\}_{K_R}$。

由上式及 B1、A5 可得 S CanProve R Claim K。

由上式、式(14) 及 A5 可得：

S CanProve R Claim M (17)

由式(9) 及式(17) 可知，改进后的协议其 *EOO* 及 *EOR* 的设计符合可追究性的要求。

③ 分析协议是否达到可追究性目标：

因为 $O_R^3=O_R^2\cup EOO$, $O_S^4=O_S^3\cup EOR$。我们有：$EOO\in O_b^3\subseteq O_b$和$EOO\in O_a^4\subseteq O_a$。因此，协议达到可追究性目标。

3) 公平性分析。

协议达到公平性目标等价于下述命题成立：$EOO\in O_R^{i-1}$当且仅当$EOR\in O_S^{i-1}$，其中$i=1,2,3,4$。由于协议第3) 步和第4) 步由 *TTP* 同时向 S 和 R 发出，故在弹性信道的条件下，S 和 R 总可以接收到 *EOO* 和 *EOR*。所以，在弹性信道的条件下，本协议是公平的。

4 与文献[6]中协议的比较

本文提出的协议能够满足挂号电子邮件协议的安全性要求，与文献[6]中的协议比较，本文具有以下几个优势：

1) 添加了消息 M4，该消息能够真正使得发送方获得收方的不可否认证据。

2) 消息 M4 中的内容在步骤2) 中由 R 签名后发送给 *TTP*，*TTP* 在验证其签名有效后发送给 S，若有效性验证无法通过，*TTP* 不会把 M3 发送给 R，R 也就无法获得邮件 M。这样避免了由 R 发送消息可能导致协议公平性受到破坏的情况。

3) 在 M3 中，消息由 *TTP* 签名，避免了其他攻击者冒充 *TTP* 发送消息来欺骗 R 的情况。

整体来看，本文的协议没有增加加密次数，其代价和文献[6] 中的协议类似。虽然比文献[6] 中的协议多了一个步骤，但由于文献[6] 中的三个步骤无法使发送方获得不可否认证据，故第四个步骤的增加是必须的，否则协议的不可否认性无法得到满足。

(下转第1935页)

时向主体发送授权消息,否则向主体发送禁止授权消息。

在本模型中,约束条件存储在授权规则数据库中,并且包含与主体变元、客体变元的状态和环境上下文信息相关的逻辑条件,而主体、客体和环境上下文信息存储在知识库中并且是实时变化更新的。因此,在授权过程中访问控制引擎在查询授权规则数据库时需要结合知识库中的主体、客体和环境上下文信息等事实,最终确定主体满足的约束条件和授权规则。

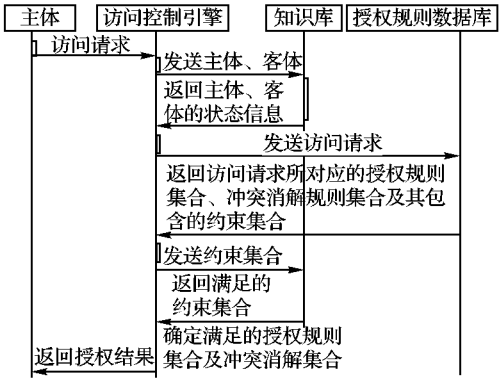

图 2　授权过程的时间序列图

4　结语

在普适计算环境下,用户能否随时随地有效访问计算资源是一个基础性问题。本文提出了一种普适计算环境下基于主体、客体状态的上下文敏感的动态访问控制模型,研究了主体对客体的四种权限类型以及主体与主体之间的四种交互权限,建立了动态授权模型的体系结构,并描述了授权算法。与目前提出的模型相比,CDACM 模型综合考虑了主客体的状态和上下文信息对授权的影响,采用统一的约束模式描述主客体状态和上下文信息,在保证模型简单性的同时有效提高了模型的表达能力和实用性;通过定义冲突消解规则和冲突消解优先偏序关系集合解决了基于系统状态的冲突消解问题,使得模型是一致的和完全的,进一步增强了模型的表达能力,更适合于普适计算环境。

参考文献:

[1] WEISER M. The computer for the twenty-first century[J]. Scientific American, 1991, 265(3): 94 - 104.

[2] 徐光祐, 史元春, 谢伟凯. 普适计算[J]. 计算机学报, 2003, 26(9): 1042 - 1049.

[3] PATRIKAKIS C, KARAMOLEGKOS P, VOULODIMOS A, *et al*. Security and privacy in pervasive computing[J]. IEEE Pervasive Computing, 2007, 6(4): 73 - 75.

[4] 郭亚军, 洪帆, 沈海波, 等. 普适计算面临的安全挑战[J]. 计算机科学, 2007, 34(6): 1 - 3, 12.

[5] SANDHU R S, COYNE E J, FEINSTEIN H L, *et al*. Role-based access control models[J]. IEEE Computer, 1996, 29(2): 38 - 47.

[6] 王小明, 赵宗涛. 基于角色的时态对象存取控制模型[J]. 电子学报, 2005, 33(9): 1634 - 1638.

[7] BERTINO E, BONATTI P A, FERRARI E. TRBAC: A temporal role-based access control model[J]. ACM Transaction on Information and System Security, 2001, 4(3): 191 - 223.

[8] BERTINO E, CATANIA B, DAMIANI M L. GEO-RBAC: a spatially aware RBAC[C]// 10th ACM Symposium on Access Control models and Technologies. Sweden: ACM, 2005: 29 - 37.

[9] YU H, LIM E P. LTAM: A location-temporal authorization model [J]. Secure Data Management, 2004(12): 172 - 186.

[10] ZHANG GUANG-SEN, PARASHAR M. Context-aware dynamic access control for pervasive applications [EB/OL]. [2007 - 08 - 23]. http://citeseer.ist.psu.edu/687356.html.

[11] KAGAL L. Rei: A policy language for the me-centric project[EB/OL]. [2007 - 08 - 26]. http://ebiquity.umbc.edu/paper/html/id/123/Rei-A-Policy-Language-for-the-Me-Centric-Project.

[12] KAGAL L, FININ T, JOSHI A. A policy language for a pervasive computing environment[C]// 4th IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY'03). USA: IEEE Computer Society, 2003: 63 - 74.

[13] LAPU E C, SLOMAN M. Conflicts in policy-based distributed systems management[J]. IEEE Transactions on Software Engineering, 1999, 25(6): 852 - 869.

[14] DUNLOP N, INDULSKA J, RAYMOND K. Methods for conflict resolution in policy-based management systems[C]// 7th International Conference on Enterprise Distributed Object Computing. Washington DC: IEEE Computer Society, 2003: 98 - 109.

(上接第 1930 页)

5　结语

本文分析了文献[6]提出协议的缺陷,提出了一个基于在线第三方的挂号电子邮件协议。通过对本文提出的协议进行的扩展 Kailar 逻辑分析可以看出,该协议具有挂号电子邮件所需要的保密性、不可否认性及公平性。同时协议还具有抗篡改、重放等攻击,及第三方无法获得邮件的内容的优点。

参考文献:

[1] BRUCE S, JAMES R. A certified E-mail protocol[C]// The 13th Annual Computer Security Applications Conf(CSAC'97). San Diego: IEEE Computer Society, 1998: 347 - 352.

[2] ABADI M, GLEW N. Certified E-mail with a light on-line trusted third party: Design and implementation[C]// The 11th International World Wide Web Conference (WWW'02), Honolulu, Hawaii, USA: ACM Press, 2002: 387 - 395.

[3] DENG R H, GONG L, LAZAR A A, *et al*. Practical protocols for certified electronic mail[J]. Journal of Network and Systems Management, 1996, 4(3): 279 - 297.

[4] ASOKAN N, SHOUP V, WAIDNER M. Asynchronous protocols for optimistic fair exchange[C]// IEEE Symposium on Research in Security and Privacy, Oakland. USA: IEEE Computer Society, 1998: 86 - 99.

[5] ZHOU JIANYING, DENG R H, BAO F. Some remarks on a fair exchange protocol[C]// PKC'2000. Australia: Springer - Verlag, 2000. 46 - 57.

[6] 彭红艳, 李肖坚, 夏春和, 等. 一种面向电子邮件的不可否认协议及其形式化分析[J]. 计算机研究与发展, 2006, 43(11): 1914 - 1919.

[7] KAILAR R. Accountability in electronic commerce protocols[J]. IEEE Transactions on Software Engineering, 1996, 22(5): 313 - 328.

[8] 卿斯汉. 一种电子商务协议形式化分析方法[J]. 软件学报, 2005, 16(10): 1757 - 1765.