电子商务协议研究综述*

周龙骧

(中国科学院 数学与系统科学研究院 数学研究所,北京 100080)

E-mail: lxzhou@math08.math.ac.cn

http://www.amss.ac.cn

摘要: 电子商务协议是电子商务实施的技术基础.对电子商务协议研究进行综述,包括电子商务协议设计的原则(如安全性、匿名性、原子性、不可否认性和交易规模)以及对若干著名电子商务协议的描述和分析.

关键词: 电子商务;电子商务协议;安全性;匿名性;原子性;不可否认性;交易规模

中图法分类号: TP309 **文献标识码**: A

冲绳八国集团发表的全球信息化宣言其核心内容之一即是电子商务(electronic commerce).据 IDC 预测,全球电子商务的规模 1998 年为 375 亿美元,到 2003 年将突破一万亿美元,2004 年将达到 7.29 万亿美元."上网的企业不一定能成功,但不上网的企业将迟早被淘汰出局"已成为大多数人的共识.

世界上许多举足轻重的大企业已将电子商务列为主要的发展方向.IBM 公司 1/4 的收入约 200 多亿美元来自 e-business.它向 1.2 万家公司采购,电子商务使其在 2000 年节约 18 亿美元.网络巨人 Cisco 公司 85%的交易在线完成,网上销售每日 5 000 万美元,电子商务使其销售额增长 500%,而人员仅增加 10%,交货期由 3 周降为 3 天,客户满意度上升 52%.Dell 公司每日网上销售 5 000 万美元,Web 收入超过 50%.Intel 公司每月网上交易逾 10 亿美元,占收入 42%.Oracle 公司已近 100%实现在线销售,年节约 10 亿美元.施乐、通用汽车、万事达信用卡这 3 家公司采用在线采购后,成本分别下降了 83%,90%和 68%.

国内电子商务公司自 1999 年下半年以来每日增加两家,已逾 300 家公司.中国人民银行已建成全国认证中心(Certificate Authority),为电子商务提供了权威的第三方.

总的看来,美国电子商务的启动期为 1992~1995 年,1995~1999 年为其高速增长期,从 2000 年开始已进入了稳定成长期.我国的电子商务相对滞后,1995~1999 年为启动期,从 1999 年起开始进入高速增长期.2000 年纳斯达克的缩水是市场的正常调整,挤尽泡沫之后将会有更健康的发展.

1 电子商务平台

电子商务是网络经济和知识经济的主要内容之一.它影响到整个人类社会的生活,涉及面很广,包括政治、经济、法律、伦理道德、社会学、金融、商业、政府、社区组织等.在技术层面关系到过程工程、软件工程、系统集成、信息安全和密码学、网络技术、数据库技术、多媒体等.电子商务系统是数据库、Web 服务器、商务应用软件、网络安全、网络服务等的汇集,技术复杂,这为各大 IT 企业,特别是数据库厂商提供了机会,充分发挥了它们的商业和技术优势.IBM 公司的 Websphere Commerce Suite 利用其 DB2 数据库系统提供全面的电子商务解决方案.微软公司基于 Windows 2000 和 SQL Server 提供 Web Site,MS Market,MS Sale 和 MS Expense 全套软件.Oracle 公司以 Oracle 9i 为基础,提供电子商务套件:Oracle iStore,Oracle iMarketing,Oracle iPayment,以及企业内部管理 ERP、客户关系管理 CRM 和供应链管理软件 SCM.CA 公司以 Unicenter TNG,Jasmine ii,Neujent 为基础推出全套电子商务平

* 收稿日期: 2001-02-16; 修改日期: 2001-05-21

基金项目: 国家自然科学基金资助项目(69983011)

作者简介: 周龙骧(1938-),男,浙江瑞安人,研究员,博士生导师,主要研究领域为分布式数据库系统,多媒体数据库系统,电子商务.

台. SUN-Netscape 公司有 iPlanet,iForce. Informix 公司有 iReach,其电子商务软件 iSell 获得了英国 Network News & Miller Freeman 的 Internet/Web 奖. Intel 公司有 e-Provider. HP 公司有 net-Channel. SGI 公司有 Media Commerce. Sybase 公司有 Enterprise Portal,Mobile & Wireless 电子商务以及 Vertical Solution 电子商务解决方案. Lotus 公司有 e business 和 e-Collaboration.

国内的 IT 企业也推出了拥有自主版权的电子商务平台.如,用友公司推出了新世纪版电子商务应用软件,包括财务、供应链管理、客户关系管理、人力资源管理、制造、决策支持等;实达公司推出了 iHome,iCom 和 iPro;东大阿尔派公司有成套的 Neteye,iProcument,iCRM,iDRP 和 Openflow 等;8848 公司有网上交易市场 e-Marketplace;联想、方正、中软等公司也都有自己的解决方案.

2 电子商务研究

相对于 IT 企业大手笔的工具、平台和解决方案,学术界在电子商务的研究方面则稍显落后,不得不急起直追,各顶级学术会议,如数据库界的 VLDB,SIGMOD,DEXA,Data Engineering 等都专辟电子商务的课题,专题的电子商务学术会议也如火如荼.从 1997 年 7 月～1998 年 6 月,一年间此类会议举办了 18 次之多. 1998 年 8 月纽约举行的第 24 届 VLDB 会议以电子商务为重点[1];SIGMOD Record 出了电子商务的专辑(1998 年 12 月)[2]. 2000 年 9 月 DEXA 在英国伦敦 Greenwich 召开了第 1 届国际电子商务和 Web 技术会议[3].这一切表明了学术界对电子商务的重视.电子商务的研究方兴未艾.

电子商务的研究范围十分广泛,以下是其中的一些课题:

(1) 电子商务系统的体系结构研究,如基于部件(component-based)的电子商务系统和基于智能代理(agent-based)的电子商务系统[2].

(2) 电子商务的原子性(atomicity)和协议研究,如包括满足 3 种原子性的 Netbill 协议;只满足钱(money)原子性的 SSL,SET 和 First Virtual 协议;不满足任一原子性的 Digicash 协议等[2].

(3) 支持网络经济的新技术 XML 的研究和标准化[4-10].

(4) 采购协议(procument protocol)、支付协议、物流配送协议和交换协议的研究.

(5) 信息流、资金流和物流中的安全.

(6) 拍卖(auction)和协商(negociation)技术.

(7) 密码技术.

(8) 数字产品.

(9) 电子出版.

(10) 供应链、联盟(coalitions)和虚拟企业模型.

(11) 新型商业模型.

(12) 知识产权保护.

(13) 描述商品、服务和合同的语言.

(14) 网上估价(pricing)和竞价.

(15) 名誉和信用机制(reputation and trust).

(16) 电子商务标准化.

(17) 电子商务中的移动 Agent.

(18) 客户保护.

(19) 实例研究.

(20) 电子商务的应用领域(保健、旅游、贸易、教育、政府、运输和后勤).

(21) 服务质量(QoS).

(22) 社会、组织和跨文化课题.

3 电子商务协议

3.1 电子商务模型

电子商务是客户(customer)、商家(merchant)、银行(bank)和为各方所信任的第三方认证机制(CA)之间的信息流、资金流和物流的交互关系.各方是通过遍及全球的、开放的但不安全的 Internet 相互联系的,如图 1 所示.

3.2 电子商务协议

在电子商务模型中,四方三流交互关系必须有规可循,以保证各方利益和安全,并能控制风险,这就是各种协议(protocol).

协议有不同的规定,从而有不同的复杂性、不同的开销、不同的安全和不同的风险.

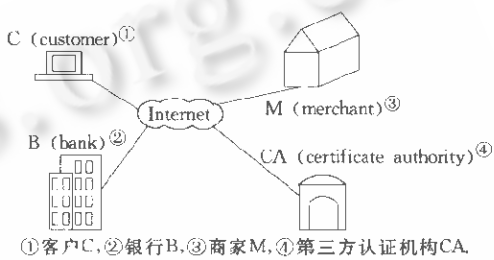


Fig. 1 Electronic commerce model
图1 电子商务模型

下面,我们来看一个著名的 Digicash 协议的例子[11~13]:

(1) 顾客 C 从银行 B 取款,收到可当钱用的加密的代币 Token.

(2) 顾客对该代币作密码变换,使商家 M 能够验证该代币的有效性,但已不能追踪顾客 C 的身份.

(3) 顾客以该代币在商家 M 处购物,为此,她(本文遵循文献惯例,对弱势的顾客用"她",而对商家则用"他")进一步作密码变换,将商家 M 的标识纳入采购数据之中.

(4) 商家 M 检验顾客 C 提交的代币(已不能追踪顾客 C 的标识),确认此前未收到过该代币.

(5) 商家 M 发货给顾客 C.

(6) 过后,商家到银行 B 兑现所收到的电子代币.

(7) 银行 B 检验该代币的唯一性(即未曾花费过).若是唯一的,则付款或转帐给商家 M,顾客 C 的身份仍保密,未被泄露;否则,该电子代币已再次花费,则顾客 C 的身份将被暴露,其匿名性不能保持,并将通知网络警察追究花费者的欺诈罪.

以上协议简单、易行,保证了电子交易的顺利进行,保证了各方的利益,保护了顾客所希望的匿名性.

现在我们考虑一种例外情况,若在交易的第(3)步通信发生故障(对因特网来说是经常的),此时顾客 C 无法确定她所付出的电子代币 Token 商家 M 是否收到?

顾客 C 有两种选择:

(1) 将代币 Token 退还给银行 B,或到另一商家 M′处购物.这时默认了商家 M 未收到该代币.但若事实上商家 M 已收到了该代币,则此选择将导致顾客 C 重复使用该代币而丧失了匿名性,而且还会被指控欺诈.

(2) 顾客 C 不采取行动.这时默认了商家 M 收到了该电子代币.但若事实上商家 M 未收到该代币 Token,则此选择将导致顾客 C 受到损失,她既收不到所购的商品也未能使用该代币.

因此以上的 Off-Line Digicash 协议是有缺陷的(为此,Digicash 协议的商业版采用了全 On-Line 方式).

上述例子说明,在电子商务协议的设计中可能出现问题,需要进行研究.

4 电子商务协议的设计原则

不同的电子商务协议在方便性、安全性、风险等方面是不同的,不同的应用环境对协议目标的要求也不相同.下面,我们列出电子商务协议设计时的若干原则,可以作为设计时的参照.

4.1 匿名性(anonymity)

由于种种原因,客户在商业交易中常常希望保护自己的隐私,不愿泄露自己的身份、购物习惯、购物品种和数量等信息.在现金交易中一般可以很有效地保护客户的身份.钞票虽有号码,但通常不会暴露使用者是谁.Digicash

协议的设计即考虑了保护客户的匿名性.

匿名性虽然是一种商业交易中的需求,但也有其负面影响,许多国家将匿名交易定为非法.如美国的反洗钱法Money Laundering Act(12 USC § 1829)规定电子商务系统必须保证:

· 立即报告任何价值超过一万美元的交易;

· 记录任何价值超过100美元的交易.

一种可行的折衷办法是通过可信任的采购代理来购物,客户的身份等私有信息保存在代理处,追踪也仅仅追到代理为止[14].

4.2 安全性(security)

安全性是电子商务协议中最重要的性质,一个不安全的协议是不会为人们所接受的.但是,越高的安全性其开销越大,代价越高.因此,设计电子商务协议时应针对不同的应用需求,给出不同程度的安全安排.生活中常有的微交易(micro transaction),仅涉及几元、十几元的小额支付或微支付(micro payment),如电话费、查询费等,需设计低开销的安全措施.

从技术上说,当前的信用卡方式(也是一种电子商务协议)是不安全的.比如,参加国际学术会议被要求预付注册费,将客户的信用卡号和签名通过邮件或因特网发送,很容易被窃取.又如,使用信用卡时将顾客的卡号、付款数、签名暴露给商家,易造成商家欺诈.1997年7月到1998年6月,14 600名美国和加拿大游客在墨西哥旅游,信用卡损失达2 500万美元,其中餐馆占19.7%,自选市场占21%.商家欺诈是信用卡交易面临的最大问题之一.

电子商务涉及各方的相互信任问题,它与安全性关系密切.有的协议假定信任某个第三方[15,16],有的协议则假定不信任有关方[17].

4.3 不可否认性(nonrepudiation)

电子商务有关各方通过因特网进行交易.由于供需双方不会谋面,因此,确保各方承诺的不可否认性十分重要.电子商务中最为普遍的技术是通过数字签名(digital signature)来确保各方所发出信息的不可抵赖性[18].

4.4 原子性(atomicity)

事务(transaction)的原子性原本是数据库领域中的概念[19~21],是指对数据库操作的一个逻辑单元,该单元由一系列操作组成.事务将数据库从一个一致的相容状态(consistent state)转换为另一个一致的相容状态:

Transaction Begin

操作1;

操作2;

⋮

操作n;

Transaction End

事务的原子性是数据库最根本的概念之一.推而广之,T. D. Tygar[1,22~25]在电子商务中引入了原子性的概念,以规范电子商务中的资金流、信息流和物流.Tygar的原子性分为3级,呈向上兼容关系,后者包含前者.

4.4.1 钱原子性(money atomicity)

钱原子性定义为电子商务中的资金流守恒,即资金在电子商务有关各方的转移中既不会创生也不会消失.例如,现金交易是满足钱原子性的,购买者钱的减少等于销售者钱的增加.

第3.2节中的Digicash协议则不满足钱原子性.在通信发生故障时,协议本身不能保证钱原子性,也使客户的匿名性丧失.

4.4.2 商品原子性(goods atomicity)

商品原子性的定义如下:首先,满足商品原子性的协议一定是满足钱原子性的;其次,必须保证购买者如果付了款就一定会得到商品,购买者如果得到了商品则一定付了款,不存在付了款而得不到商品或者得到了商品而未曾付款的情况.如易国(eguo)和卓越网的送货上门,货到付款的方式就是一种满足商品原子性的协议.Digicash协

议显然不满足商品原子性.

商品原子性对于经由因特网发售的信息商品或数字商品,如软件、音乐、电影等,具有特别重要的意义.

4.4.3 确认发送原子性(certified delivery)

确认发送原子性的定义如下:首先,满足确认发送原子性的协议一定满足钱原子性和商品原子性;其次,需要有对客户购买的和商家销售的商品的内容及品质的双方确认,亦即满足确认发送原子性的协议必须同时保证购买者得到她所订购的商品(包括品质),商家发送了客户订购的商品.

为了达到确认发送原子性,可以通过一个可信任的第三方,也可以从技术上来保证.在下面的实例中将介绍满足确认发送原子性的电子商务协议.

确认发送原子性对于客户和商家互不信任的场合特别有意义,满足此原子性的协议可让客户和商家双方认可所发送商品的内容和品质.

4.5 交易规模(transaction size)

在发达国家如美、日、欧,每次信用卡交易的规模平均价值约为50美元,每次交易的费率由商家负担,约为30美分加上商品价格的2%.若为电话订购或邮购,则实际费率约为50美分加上商品价格的2.25%.

交易规模很小的交易,例如小于1美元的交易,通称为微交易(micro transaction)或小额交易.其交易费率应作特殊的设计,否则,商品或服务的价格将由信用卡的费率所主宰,这显然是不合适的.应该设计和开发特定的优化的电子商务协议,以支持微交易[24,26].

5 若干著名的电子商务协议

5.1 加密(cryptograph)[27]

为了行文方便,首先简单引入加密的若干记法:

SK	秘密密钥(私钥)	秘密
PK	公开密钥(公钥)	公开
E	加密变换	公开
D	解密变换	公开
p,q	素数	秘密
$r=p\cdot q$		公开
$\varphi(r)=(p-1)(q-1)$		秘密
X	明文	秘密
Y	密文	公开

我们有[18,28]

$$\mathrm{PK}\cdot\mathrm{SK}=\mathrm{SK}\cdot\mathrm{PK}\equiv 1(\mathrm{mod}\ \varphi(r)),$$
$$E_{\mathrm{PK}}(X)=Y,$$
$$D_{\mathrm{SK}}(Y)=X,$$
$$D_{\mathrm{SK}}(E_{\mathrm{PK}}(X))=E_{\mathrm{PK}}(D_{\mathrm{SK}}(X))=X(\mathrm{mod}\ r).$$

5.1.1 公开密钥基础结构(public key infrastructure,简称PKI)

由R. Rivest, A. Shamir和L. Adleman[18]提出的加密方法,只有用于解密的私钥SK是保密的,其余用于加密的公钥PK、加密算法E和解密算法D都是公开的.由于加密密钥与解密密钥不同,故亦称为不对称加密.

5.1.2 对称加密

如果加密密钥和解密密钥相同,则称为对称加密.最著名的对称加密是美国国家标准局的数字加密标准DES(data encryption standard).它于1975年提出并生效,1980年成为ANSI标准.通常DES密钥长56位,但已被破译,必须用更长的密钥,如128位.改进的算法是三层加密标准3DES(triple data encryption standard),而最新的正在制定的是美国国家标准与技术局NIST(National Institute of Standards and Technology)的先进加密标准AES

(advanced encryption standard).

利用PKI的RSA算法可以方便而高效地实现信息加密和数字签名.

设A欲向B发送信息X,A利用公开的B的公钥PKB将X加密:

$$Y=E_{PKB}(X),$$

然后将密文Y经由开放的因特网发送给B.由于解密的私钥SKB只有B才知道,故不必担心因中途被截而泄密.

B收到Y后利用SKB将Y解密,得到明文X:

$$X=D_{SKB}(Y)=D_{SKB}(E_{PKB}(X)).$$

数字签名是为了保证信息确为发送者所发而设定的.设A欲发送信息X给B,A可通过数字签名表明所发信息确为自己所发,即利用只有A才知道的私钥对X加密:

$$Y=D_{SKA}(X),$$

然后将已加密的Y发送给B.B收到后,利用公开的A的公钥PKA将Y解密:

$$X=E_{PKA}(Y)=E_{PKA}(D_{SKA}(X)),$$

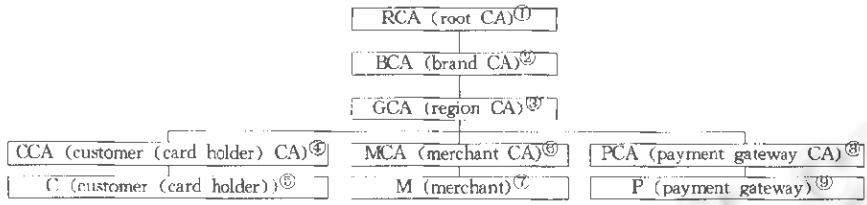
即可确定所收到的X必为A所发.

在实践中,加密和数字签名经常结合起来使用.

5.2 认证和认证中心(certification and certificate authority)

为了彼此确认因特网上打交道的对方,必须由权威的第三方来给出认证.正如客户在银行存款或取款必须出示自己的身份证,而该身份证是由大家信任的第三方公安局所给出的一样.在电子商务中,权威的第三方称为认证中心.它是一个权威而非权力机构,如美国的Verisign公司和我国的中国金融认证中心CFCA.

认证中心发放和管理数字证书,一般为一种树形结构,最权威的是根认证中心,如图2所示.



①根认证中心RCA,②品牌认证中心BCA,③区域认证中心GCA,④持卡人认证中心CCA,⑤持卡人C,⑥商家认证中心MCA,⑦商家M,⑧支付网关认证中心PCA,⑨支付网关P.

Fig. 2 Tree structure of certificate authority
图2 认证中心的树型结构

在验证发生疑问时,可循上图逐级往上,直至RCA.RCA发放品牌证书所使用的数字签名密钥一般为2 048位,BCA发放品牌证书所用数字签名密钥为1 024位,往下逐级减少密钥的位数.显然,位数越多就越安全、可靠,但开销也就越大.

5.3 安全套接层协议SSL(secure socket layer)

安全套接层协议SSL是目前使用最为广泛的电子商务协议.它由Netscape公司设计开发,由于内置于用户浏览器和商家的Web服务器中,故能方便而低开销地进行信息加密,多用于信用卡号的传送.它相当于在客户和商家之间建立一条保密通道连接,以传送信用卡号等信息.SSL协议如下:

(1) 客户C与商家M建立连接.

(2) 商家M向客户传送自己的数字证书.

(3) 客户C利用浏览器中的SSL软件随机产生传输密钥,以商家的公钥加密后传送给商家.

(4) 客户将自己的信用卡号用传输密钥加密后传送给商家.

SSL协议只保证在信息传送过程中不因被截而泄密,但不能防止商家利用获取的信用卡号进行欺诈[29].此外,商家的服务器也不能保证安全.它满足钱原子性.

SSL协议对商家进行了认证,但未对客户进行认证(也许是一个黑客,也许是在洗钱,也许是盗窃的信用卡,也

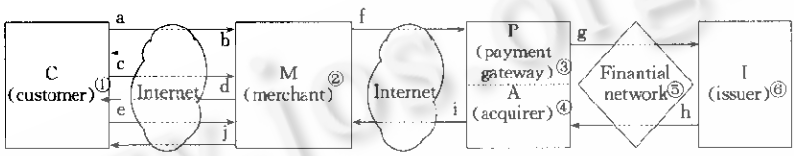
许是抵赖订货),这应予注意.

5.4 安全电子交易协议 SET(secure electronic transaction)

安全电子交易协议 SET 是 Mastercard 公司和 Visa 公司于 1996 年联合开发的[30],此前有 Mastercard, Netscape, IBM 公司的安全电子支付协议 SEPP(secure electronic payment protocol)以及微软和 Visa 公司的安全交易技术 STT(secure transaction technology). 1997 年, Mastercard 和 Visa 公司成立了 SETCO 公司,负责根认证机构 RCA 的管理(由 American Express 和 JBC Credit Card Company 提供支持). 品牌证书及其以下的证书由 Mastercard 和 Visa 公司委托 Verisign 和 GTE 建立认证中心进行管理,数字证书符合 X.509 标准.

SET 协议是一个比较复杂的协议,其协议的描述有数百页之多. 它可以对交易各方进行认证,可防止商家欺诈,进行安全交易,但开销较大,客户、商家、银行都要安装相应的软件.

SET 协议的描述如图 3 所示.



①客户C,②商家M,③支付网关P,④收单行A,⑤金融专网,⑥发卡行I.

Fig. 3 SET protocol flow chart

图3 SET协议流程

(1) 客户 C 向商家 M 发出采购请求(图 3 中的消息 a).

(2) 商家 M 向客户 C 报价(目录清单)(图 3 中的消息 b).

(3) 客户 C 同意报价,并对订单 OI(order instructions)进行数字签名:

$$OI' = D_{SKC}(OI),$$

然后将 OI′发给商家 M(图 3 中的消息 c).

(4) 商家 M 对收到的 OI′解密:

$$OI = E_{PKC}(OI').$$

确认订单 OI 为客户 C 所发.

商家对自己的数字证书 Cer_M、支付网关的数字证书 Cer_P(事先储存在商家 M 的服务器中)以及付款要求 Pay 进行数字签名:

$$Y = D_{SKM}(Cer_M, Cer_P, Pay),$$

然后发给客户 C(图 3 中的消息 d).

(5) 客户 C 收到 Y,对 Y 进行解密:

$$(Cer_M, Cer_P, Pay) = E_{PKM}(Y),$$

确认 Y 为 M 所发,确认商家 M 和支付网关 P 的身份.

客户 C 生成按 Pay 要求的支付命令 PI(payment instructions),并进行数字签名:

$$PI' = D_{SKC}(PI).$$

客户 C 取随机生成的一个对称密钥 K,由 K 对 PI′进行加密:

$$PI'' = E_K(PI').$$

对客户 C 的帐户信息 PAN(C 的姓名、信用卡号等)和 K 用支付网关 P 的公钥进行加密:

$$P1 = E_{PKP}(PAN, K).$$

以上两步加密防止了商家 M 获悉有关客户 C 支付的信息,只有支付网关 P 才能解密.

对客户 C 的数字证书 Cer_C,PI″及 P1 进行数字签名:

$$Y1 = D_{SKC}(Cer_C, PI'', P1),$$

然后发给商家 M(图 3 中的消息 e).

(6) 商家 M 对收到的 Y1 进行解密：

$$(Cer_C, PI'', P1) - E_{PKC}(Y1),$$

确认为客户 C 所发.

对 Cer_C, PI'', P1 和商家 M 自己的数字证书 Cer_M 进行数字签名：

$$Y2 = D_{SKM}(Cer_M, Cer_C, PI'', P1),$$

然后发送给支付网关 P(图 3 中的消息 f).

(7) 支付网关 P 对收到的 Y2 进行解密：

$$(Cer_M, Cer_C, PI'', P1) = E_{PKM}(Y2),$$

确认为商家 M 所发.

对 P1 进行解密,确认为客户 C 所发信息：

$$(PAN, K) = D_{SKP}(P1).$$

利用其中的对称密钥 K 对 PI''进行解密：

$$PI' = D_K(PI''),$$

再对所得到的 PI'进行解密：

$$PI - E_{PKC}(PI'),$$

获得曾由客户 C 数字签名的支付命令 PI.

将支付命令 PI 经由安全的金融专网发给发卡行 I(图 3 中的消息 g).

(8) 发卡行 I 进行验证,确认客户 C 的帐号有效(有足够余额). 然后将经验证有效的支付命令 PI 经由金融专网发还给支付网关 P(图 3 中的消息 h),客户帐号和商家帐号间发生资金划拨(这不是由 SET 协议规定的).

(9) 支付网关 P 向商家 M 发支付已讫消息 M_{sg}(图 3 中的消息 i)：

$$M'_{sg} = D_{SKP}(M_{sg}).$$

(10) 商家 M 对收到的 M'_{sg}进行解密,确认为支付网关 P 所发：

$$M_{sg} = E_{PKP}(M'_{sg}),$$

商家 M 向客户 C 发货(图 3 中的消息 j).

综上所述:客户 C 要验证商家 M 的数字证书、支付网关 P 的数字证书以及商家 M 所发的付款请求. 商家 M 要验证客户 C 所发的订单 OI、客户 C 的数字证书、客户 C 所发的消息 Y1 以及支付网关所发的消息 M_{sg}. 支付网关 P 要验证商家 M 所发的消息 Y2、商家 M 的数字证书、客户 C 的数字证书以及客户 C 所发的支付命令 PI. 发卡行 I 要验证客户 C 的帐号有效.

从以上描述可知,在 SET 协议中,客户、商家、银行的身份要互相认证. 客户 C 的订货信息只有商家 M 知晓,银行并不知道,而客户 C 的信用卡号等信息商家 M 并不知道,从而防止了信用卡交易中的商家欺诈.

在 SET 协议的消息交流中采用数字签名的办法,因而有效地防止了任一方的抵赖,也确认了消息发送者的身份.

SET 协议显然满足钱原子性,但并不满足商品原子性和确认发送原子性.

虽然 SET 协议与 SSL 协议相比具有上述优点,但 SET 协议复杂,开销大,代价高. 协议各方包括客户必须安装相应的软件,这有碍于它的普及和流行. 一种折衷的办法是,在客户和商家之间采用 SSL 协议,而在商家和银行之间采用 SET 协议.

在以上对 SET 协议的描述中,尚可采用若干变通的办法以减低开销. 例如,在第(5)步中生成的对称密钥 K 用于对支付命令 PI 进行加密,其实,省略这一步,直接用支付网关 P 的公钥 PKP 对 PI 进行加密也是可行的,当然,其安全程度较原来方法有所不同,且加工效率亦不相同. 通常 DES 算法的效率比 RSA 算法的效率要高 1 000 倍[27].

5.5 匿名原子交易协议(anonymous atomic transaction protocol)

第 3.2 节讨论的匿名数字现金协议 Digicash 不能满足最基本的钱原子性. J. D. Tygar 等人首次给出了兼有匿名性和原子性的电子商务协议[31]. Tygar 将传统的分布式系统中常用的两阶段提交(two phase commitment)加以

改进,引入除客户C、商家M和银行B之外的独立的第四方——交易日志L(transaction log),以取代两阶段提交协议中的协调者(coordinator)的角色.由于协调者需要了解其他三方包括客户的身份,与客户的匿名性矛盾,故须作此改进.

客户C在银行B中有一个帐号,她可以向银行提取匿名的代币Token(blinded digitalcash).Token由客户和银行的一次性交互而产生,只有银行才能发行Token,银行不可以通过它追踪其持有者的身份.但若客户两次使用同一Token,则银行会检查出来,并揭露该客户的身份.

5.5.1 取款协议

客户C向银行B提取匿名代币的协议如下:

(1) 客户C随机生成一对取款公共密钥Q和q,其语义符合RSA的规定,然后生成提款请求:

$$M_{sg}=(C_{ACC},Q,Val),$$

其中C_{ACC}为客户C的帐号,Q为取款公钥,Val为欲提款数.

C对M_{sg}进行数字签名,然后用银行公钥进行加密,并发给银行:

$$M_{sg}1=E_{PKB}(D_{SKC}(M_{sg})).$$

(2) 银行B收到客户C发来的提款请求,解密后得到M_{sg},确认为客户C所发:

$$D_{SKB}(M_{sg}1)=D_{SKC}(M_{sg}),$$

$$E_{PKC}(D_{SKC}(M_{sg}))=M_{sg}.$$

银行从C的帐号验证有余额后生成代币Token(Q,Val).银行维护一个Token的数据库DB_T,如下所示.

Q	Val	特征位	指向C_{ACC}指针	...
...	...	...	...	

每当商家来兑现一个Token(Q,Val)时,银行首先验证其对应的特征位:若未花费过,则可将Token的值Val划转至商家的帐号,并将特征位置为已花费;若特征位为已花费,则表明是重复花费,可根据指针揭露持有该Token者的身份.

(3) 银行对Token(Q,Val)进行数字签名后发给客户C:

$$E_{PKC}(D_{SKB}(\text{Token}(Q,Val)))=M_{sg}2.$$

客户C收到$M_{sg}2$,解密后即可得到匿名代币Token(Q,Val).如果不发生重复花费Token(Q,Val),则不论是商家还是银行都不会得知Token(Q,Val)持有者的身份.

协议对银行的信用假定是:在正常情况下,亦即未发生客户多重花费同一Token的情况下,银行不会故意去暴露Token持有者的身份,即数据库DB_T的操作只有在特征位为负时才会去访问指向C_{ACC}的指针.

5.5.2 采购协议

下面给出客户使用匿名的代币进行采购的协议.这里仅涉及数字商品,如软件、音乐、电影等可以在因特网上传送的商品.

P1. 客户向商家请求购物(C→M).

P2. 商家M给客户C发送商品目录(M→C).

P3. 客户通知商家选中某项商品goods(C→M).

P4. 商家生成消息$goods_m$,以客户的公钥PKC加密后发送给客户:

$$goods_m=D_{SKM}(n,\text{Contract},E_k(\text{goods})),$$

$$M_{sg}M=E_{PKC}(goods_m).$$

其中n为商家生成的交易号;Contract包括了商品的描述及其价格;goods为数字商品,用对称密钥K加密(M→C).

P5. 客户C收到消息$M_{sg}M$后,经解密,确认为商家M所发.客户认可Contract以后即可向银行发送消息$authorization_q$,授权用Token(Q,Val)付款.

$$authorization_q=E_{PKB}(\text{Token}(Q,Val),D_q(n,\text{截止期},M,L)),$$

其中,截止期为Token(Q,Val)的有效期.超过截止期后该付款作废,客户C可用Token(Q,Val)另行消费或将其退

还给银行.客户的该项行动应在截止期后面的一段延迟期之后进行,延迟期的长度另定.对于截止期和延长期的选定,客户应与银行和商家协商确定.

消息 authorization_q 意味着客户向银行表示她准备 Commit 此项采购交易,并授权银行将代币 Token(Q,Val)的值划转给商家的帐号(C→B).

P6. 银行收到消息 authorization_q 之后,用自己的私钥 SKB 解密,得到 Token(Q,Val)和 D_q(n,截止期,M,L).读取 Token(Q,Val),得到其取款公钥 Q 和币值 Val.通过 Q 可以查 DB_T 数据库,并为 D_q(n,截止期,M,L)解密.然后,银行验证 Token(Q,Val)的有效性,确定是否存在重复花费,截止期超过与否.当确定一切有效之后,银行准备 Commit 此交易,并通知商家.银行发给商家的消息 authorization_b 是作了数字签名的,即

$$\text{authorization}_b = D_{SKB}(n,\text{截止期},M,L,Val) \quad (B\rightarrow M).$$

P7. 商家收到消息 authorization_b 以后,用银行的公钥解密,确认为银行所发,并验证交易号 n,商品价格 Val,若对截止期和交易日志 L 也无异议,商家即可准备 Commit 此次采购交易.商家向交易日志 L 发送经自己数字签名的消息:

$$\text{authorization}_m = D_{SKM}(n,\text{截止期},K) \quad (M\rightarrow L).$$

P8. 交易日志 L 收到消息 authorization_m 以后,用商家的公钥解密,确认为商家所发.L 记录 n、截止期、K 和收到时的时间戳(time-stamp),确认商家对交易 n 的提交.然后验证截止期尚未超过.当确定一切均有效之后,日志 L 决定 Commit 此次交易 n.它向客户 C 发送 Commit 消息,其中包含了商品密钥 K.同时,它也向商家和银行发送 Commit 消息.

如果 L 记录的截止期已过,则该交易 n 只能夭折.L 向客户、商家和银行发送夭折消息 Abort.

显然,L 发送的 Commit 消息和 Abort 消息都应进行数字签名,以保证安全(L→C,L→M,L→B).

P9. 客户 C 收到日志 L 发来的消息 Commit,经日志 L 的公钥解密后,确认为 L 所发,使用所包含的商品密钥 K 将 P4 步得到的 E_K(goods)解密即可得到所购买的商品 goods.客户将 goods 与 Contract 所述相比较,即可确定是否符合订购要求.

如果出现不符合要求的情况,客户可凭 Contract,E_K(goods)和 Commit 向商家索赔,或者请求第三方仲裁.

客户 C 若收到 Abort 消息,则交易 n 失败,Token(Q,Val)可重用.

P10. 商家 M 收到 L 发来的 Commit 消息,表明交易 n 已 Commit,客户已得到 goods,商家的帐号应增值 Val.若有不妥,商家可凭消息 authorization_b 和 Commit 提交仲裁.

商家 M 若收到 Abort 消息,则表明交易 n 失败,客户 C 既然得不到商品密钥 K,就无法得到 goods,商家的帐号上也不会发生资金增值.

P11. 银行 B 收到 L 发来的 Commit 消息,表明交易 n 已 Commit,银行将 Token(Q,Val)的 Val 值划转至商家的帐号.

若银行收到 Abort 消息,则表明交易 n 失败,将 Token 数据库 DB_T 中 Q 的特征位置为未花费.

5.5.3 匿名性和原子性

以上采购协议是匿名的,且满足钱原子性和商品原子性.

协议的确认发送原子性是单方的(one-sided certified delivery),即仅仅客户 C 可以确认所收到的商品的品质,而商家无法确认.若在第 5.5.2 节的采购协议中加上一步:

$$P5'.\ M_{sg}3 = E_{PKM}(D_{SKC}(E_K(\text{goods}))) \quad (C\rightarrow M),$$

即 C 将消息 $M_{sg}3$ 发送给商家 M,则商家 M 可确认客户 C 收到的是哪种商品.

5.5.4 交易日志 L

在第 5.5.2 节的采购协议中,独立的交易日志 L 必须经过客户 C、商家 M 和银行 B 的共同确认.若客户 C 和商家 M 信任银行不会与 L 串通作弊,则可将银行与 L 合并.若商家受到信任,也可以合并商家和 L.

如果客户与日志 L 串通作弊,在采购协议的 P8 步,日志不发送 Commit 消息,而只给客户 C 发送商品密钥 K,则商家将受到损失.

在上述改进的两阶段提交协议中发送消息是级联式的,即 C→M→C→M→C→B→M→L→M.它保证了原子性和匿名性.

5.6 Netbill 协议

Netbill 协议是由 J. D. Tygar 及其同事设计和开发的关于数字商品的电子商务协议[21-15,22].该协议假定了一个可信赖的第三方 Netbill Server. Netbill 协议可简述如下:

(1) 客户 C 向商家 M 发出购物请求.

(2) 商家 M 向客户 C 报价(目录清单).

(3) 客户 C 向商家 M 发送消息,表示接受该报价.

(4) 商家 M 对客户 C 订购的数字商品 G 以密钥 K 加密,然后发送给客户 C:

$$G'=E_K(G).$$

(5) 客户 C 生成一个电子采购订单 EPO(electronic purchase order),内容包括:{价格,已加密商品的加密支票(cryptographic-checksum of encryptedgoods),超时(time-out)}.

客户 C 对 EPO 进行数字签名:

$$EPO'=D_{SKC}(EPO),$$

然后发送给商家 M.

(6) 商家 M 对收到的 EPO′进行数字签名:

$$EPO''=D_{SKM}(EPO'),$$

并对密钥 K 进行数字签名:

$$K'=D_{SKM}(K),$$

然后将 EPO″和 K' 发送到 Netbill Server.

(7) Netbill Server 对收到的 EPO″和 K′进行解密,确认为商家 M 所发,再对 EPO′解密,确认为客户 C 所发,即

$$K=E_{PKM}(K'),$$

$$EPO'=E_{PKM}(EPO''),$$

$$EPO=E_{PKC}(EPO').$$

再对 EPO 中的 time-out 进行检验,确认当未过期,然后检验客户 C 的帐号,以确认有足够的资金.

当全部检验无误后即批准此次交易,将数字商品 G 的价钱从客户 C 的帐号划拨到商家 M 的帐号中.

将密钥 K 和已加密商品的加密支票存档,生成一个收据 R,对 R 和 K 进行数字签名,并发送给商家 M:

$$Y=D_{SKN}(R,K).$$

(8) 商家 M 对收到的 Y 解密,确认为 Netbill Server 所发,并验收 Netbill 签发的收据 R:

$$(R,K)=E_{PKN}(Y).$$

对收据 R 作记录.然后对密钥 K 和收据 R 作数字签名,并发送给客户 C:

$$Y'=D_{SKM}(R,K).$$

(9) 客户 C 对收到的 Y' 进行解密,确认为商家 M 所发,然后利用 K 对先前收到的加过密的 G' 进行解密,即获得所购数字商品 G:

$$G=D_K(G').$$

Netbill 协议的一个突出特征是存在一个各方信任的 Netbill Server.客户 C 与商家 M 的帐号均存于 Netbill Server 之中.

Netbill 协议的资金转移只发生在 Netbill Server 之中,客户 C 帐户资金的减少等于商家 M 帐户资金的增加,故它满足钱原子性.

Netbill 协议的第(7)步发生资金转移,它是由 Netbill Server 完成的一个原子步骤.如果在这一步之前发生通信或处理器故障,则因为未发生资金转移,也就不会发生第(8)步客户 C 收到已加密数字商品的解密密钥 K,即客

户未付款,也未收到商品的情况.若故障发生在第(7)步成功执行之后,则已发生了资金转移,密钥 K 将同时被商家 M 和 Netbill Server 保存.密钥 K 迟早会(故障恢复后)发送给客户 C,也即 Netbill 协议满足商品原子性.

Netbill 协议还满足确认发送原子性,其论证如下:

若客户 C 抱怨她收到的数字商品与所订商品品质不符,则她可将所收到的已加密数字商品 G′出示给某个仲裁者.由于商家数字签名过的密钥 K 保存于商家、客户和 Netbill Server 之中,并且已加密商品的加密支票曾由客户和商家合签,并保存于 Netbill Server 之中,因此,仲裁者即可据此检验客户 C 是否更改过所收到的数字商品以及该商品是否符合客户订购的要求.

Netbill 协议可以处理大量的微交易.研制者正与 Cybercash,Mellon Bank 和 Visa International 合作开发商品化的系统.

5.7 安全智能贸易代理协议

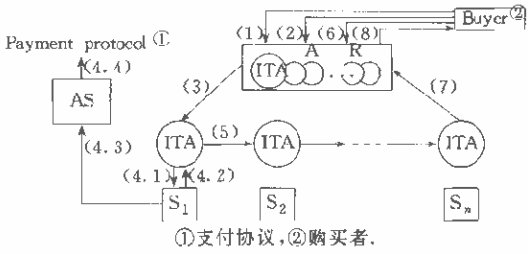
在因特网上提供的产品和服务的数量十分庞大,而且每天都在不断地增加,若采用人工方式来分析如此大量的网上产品、服务及其报价是不大可能的.于是,提出了一种智能贸易代理 ITA(intelligent trade agent)的方案.ITA 是一个软件,可在网上漫游(roam),收集与商务有关的数据(business-related),然后以持有者的立场分析这些数据并决定购买哪些产品和服务[32].与此相关的协议是由 Van der Merwe 和 Von Solms 提出的,现描述如下:如图 4所示,其中:

ITA 智能贸易代理;

AR Agent Reposity,驻留所有 Agents 的库;

AS Authorizatoin Server,在线授权服务器;

$S_1,\ldots,S_n$ 提供网上产品和服务的服务器.



①支付协议,②购买者.

Fig. 4 Van der Merwe-Von Solms protocol

图4 Van der Merwe-Von Solms协议

协议步骤如下:

(1) 购买者向 AR 出示自己的身份,以便指挥 ITA.

(2) 得到认可后,购买者指示 ITA 她要购买的商品.

(3) ITA 上网漫游,首先到服务器 S_1.

(4) ITA 搜索 S_1,若找到一种商品 item 1 符合第(2)步的指示,ITA 则决定进行交易.

(4.1) ITA 将购买者的信用卡号用 AS 的公钥加密,发送给服务器 S_1,它只能由 AS 读取.

(4.2) ITA 对选中的 item 1 进行描述,包括其价格信息,然后用 ITA 的私钥签名,再用 AS 的公钥加密,发送给 S_1.该信息仅能由 AS 读取,并必为 ITA 所写.

(4.3) S_1 对被选中的商品进行描述,包括 item 1 的价格等信息,然后将该消息用 S_1 的私钥签名,再用 AS 的公钥加密,最后将此消息和 ITA 发来的消息(第(4.2)步)一并送交 AS.

(4.4) AS 收到这两个消息后用自己的私钥解密,比较所得到的两个消息,若一致,则执行支付协议,以便将购物款划转给销售者的帐号.典型地,AS 可以是银行,通过第(4.1)步所得到的购买者的信用卡号不难完成支付协议.

(5) ITA 漫游到下一个服务器,重复以上的采购和支付.

(6) 购买者告知该 ITA 返回 AR,也可以通过第(2)步由购买者给出一定的条件,自动触发完成召回命令.

(7) ITA 返回 AR.

(8) 购买者验证该 ITA 购买了什么商品.

以上协议还存在一些不足之处:

(1) 购买者必须信任 ITA,将自己的信用卡号交给该 ITA.

(2) 授权服务器(银行)必须是在线的,才能认证和完成交易.这对可用性(availability)、连结 AS 的带宽、计算时间等都有较高的要求.

(3) AS 知道一切,不能保证匿名性. AS 知道购买者的信用卡号及身份,知道所购买的商品的性质.

5.8 具有离线授权服务器和不可信任代理的匿名电子商务协议

本协议针对第 5.7 节中的 ITA 协议进行了改进[17]. 它是匿名的,其中可信任的授权服务器是离线的,贸易代理是不可信任的.

5.8.1 秘密交换协议(secret exchange protocol)

设 A,B 双方各有 $2n$ 个秘密的 m 位的数要交换,$\{a_i,1\leqslant i\leqslant 2n\}$,$\{b_i,1\leqslant i\leqslant 2n\}$.

(1) A 将 $2n$ 个数分为 n 对,例如(a_{2j-1},a_{2j}),$j=1,\ldots,n$. 然后从每对中选一个送给 B,但 A 并不知道所选的是 a_{2j-1}还是 a_{2j},二者被选中的几率均为 1/2. 这称为 1-2 健忘传送(oblivious transfer)[33].

(2) B 也将 $2n$ 个数分成 n 对,例如(b_{2j-1},b_{2j}),$j=1,\ldots,n$. 然后从每对中选一个送给 A,也采用 1-2 健忘传送.

(3) A 和 B 互送所有 $2n$ 个数:$a_i,b_i,i=1,\ldots,2n$ 的第 1 位,然后互送第 2 位,...,直至互送第 m 位. A 要欺骗 B,其成功的几率仅为$\frac{1}{2^n}$. 因为在第(1)步 B 已经收到 $2n$ 个 a_i 中的 n 个,而 A 并不知道是 a_i 中的哪 n 个.

这种协议有一个缺陷[34]:若 A 已送出其秘密数的第 k 位之后,B 中止协议,即 B 少送一位,则 B 有 2 对 1 的好处. Tedrick 在文献[35]中解决了此问题,使先走第 1 步的一方的不利因素减至最小.

5.8.2 安全合同签字协议(secure contract signing)

(1) ITA 随机生成 $2n$ 个对称密钥(DES-like)$K_i^a(i=1,\ldots,2n)$及 n 对消息$(L_j^a,R_j^a)(j=1,\ldots,n)$. 然后对此 n 对消息进行加密:

$$P_j^a=E_{K_j^a}(R_j^a),\ j=1,\ldots,n;$$

$$Q_j^a=E_{K_{n+j}^a}(L_j^a),\ j=1,\ldots,n.$$

(2) 服务器 S 也同样随机生成 $2n$ 个对称密钥 $K_i^s(i=1,\ldots,2n)$及 n 对消息$(L_j^s,R_j^s)(j=1,\ldots,n)$. 然后对此 n 对消息进行加密:

$$P_j^s=E_{K_j^s}(R_j^s),\ j=1,\ldots,n;$$

$$Q_j^s=E_{K_{n+j}^s}(L_j^s),\ j=1,\ldots,n.$$

(3) ITA 和 S 协商一个合同,当且仅当 ITA 能解密 P_j^s 和 $Q_j^s(1\leqslant j\leqslant n)$并且 S 能解密 P_j^a 和 $Q_j^a(1\leqslant j\leqslant n)$.

(4) ITA 和 S 按照第 5.8.1 节中的秘密交换协议交换双方的对称密钥 K_i^a 和 $K_i^s(i=1,\ldots,2n)$.

5.8.3 具有离线授权服务器和不可信任代理的匿名电子商务协议

协议的步骤如图 5 所示.

(1) 客户按第 5.5.1 节中的办法向银行提款,得到匿名代币 Token(Q,Val).

(2) 客户和 ITA 按第 5.8.2 节所述的安全合同签字协议签一份合同,内容包括欲购商品的属性、价格范围、品质要求等,亦可包括 ITA 返回 AR 的条件.

(3) 客户将 Token(Q,Val)交给 ITA.

(4) ITA 漫游至服务器 S_1.

(5) ITA 按第(2)步的客户要求查找,当找到一个符合条件的商品 item 1 时即开始交易:

(5.1) ITA 和 S 按安全合同签字协议签定一份合同,合同中指明交易条件,包括 item 1 号、价格、付款、发货等.

(5.2) ITA 将 Token(Q,Val)发送给 S_1.

(5.3) S_1 向 ITA 发送 item 1.

(6) ITA 漫游至下一个服务器,重复第(5)步.

(7) 客户告知 ITA 返回 AR,亦可通过第(2)步的预置条件的触发而返回.

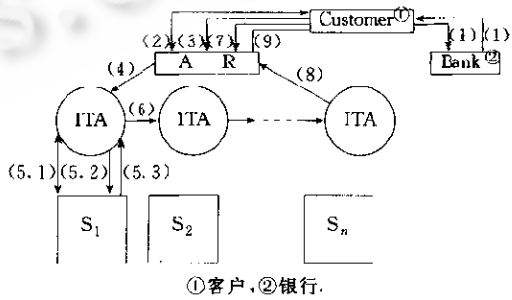


Fig. 5 New anonymous ITA protocol

图5 新的匿名ITA协议

(8) ITA 返回 AR.

(9) 客户检验该 ITA 采购的商品.

在本协议中,客户保持了匿名性,不必将信号卡号交给 ITA,在交易进行期间 AS(授权服务器或银行)不必在线.

5.9 基于 PKC 的安全电子软件分销协议

匿名原子交易协议、Netbill 协议等可以保证数字商品网上销售的原子性,但不能防止客户将购得的软件转给非授权的用户.据统计,1998 年全球软件的侵权损失达 110 亿美元,使用中的软件 38%以上为非法拷贝[36].因此,研究防止软件侵权的协议具有重要的实际意义.

5.9.1 基于 PKC 的安全电子软件分销协议

S.-M. Lee 等人[37]提出了一种基于 PKC 的安全电子软件分销协议(secure electronic software distribution protocol based on public key cryptography).它使用电子许可证 ELC(electronic licence certificate)和验证代理 AA (authentication agent)来防止软件侵权和非法拷贝.当有非法拷贝的情况发生时,商家可根据电子许可证追究原来许可的拥有者的责任.

电子许可证 ELC 由商家 M 经由因特网发送给客户 C,它包含 3 部分:

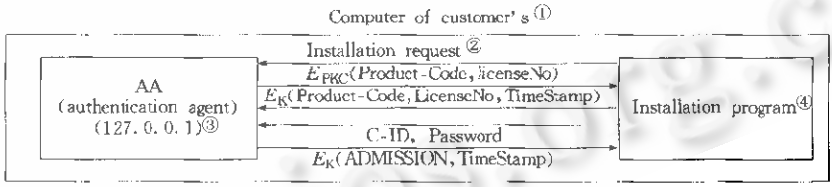
$$H(\text{Secret},\text{C-ID},\text{Password}),$$

$$D_{SKM}(E_{PKC}(\text{Product-Code},\text{LicenseNo})),$$

$$D_{SKM}(\text{Product-Code},\text{LicenseNo}).$$

其中 H 是 Hash 加密函数;Secret 为一个随机串,存储在验证代理 AA 之中,仅有 AA 和商家 M 知道;C-ID 是客户标识;Password 为口令;产品号和许可号在第 2 部分中由客户的公钥加密并由商家数字签名,在第 3 部分中由商家数字签名.

验证代理 AA 随数字商品一起发送给客户,驻留在客户的计算机中,它使用循环地址(loopback address(127.0.0.1))和预定义门户(port).AA 不仅验证客户对数字商品的安装,而且也验证数字商品的运行.数字商品的安装过程如图 6 所示.



①客户计算机,②安装请求,③验证代理AA,④安装程序.

Fig. 6 Secure installation procedure

图6 安全安装过程

(1) 当客户执行安装程序时,首先通过循环地址和预定义门户与验证程序 AA 连接,然后给 AA 发送一个安装请求.

(2) AA 用商家 M 的公钥解密电子许可证的第 2 部分,得到 E_{PKC}(Product-Code,LicenseNo)并发送给安装程序.

(3) 安装程序用客户私钥解密所收到的消息,得到(Product-Code,LicenseNo),并同时解密 ELC 的第 3 部分,将二者进行比较,若相同则继续进行.安装程序生成一个时间戳,以防止重放攻击(replay attack).初始化时有一个对称密钥 K 装入 AA 和安装程序,此时安装程序将(Product-Code,LicenseNo)和 Time Stamp 放在一起,用 K 加密后送给 AA.

(4) 安装程序将客户 C 在商家注册的客户标识 C-ID 和口令发给 AA.

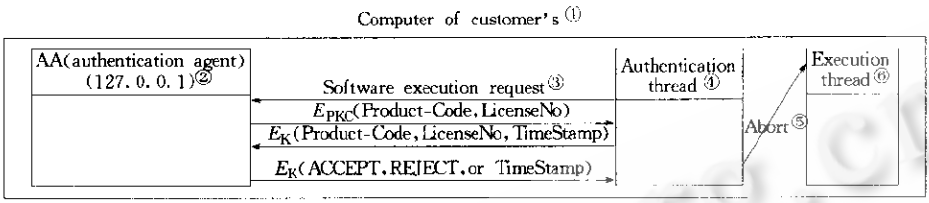
(5) AA 将收到的 C-ID,Password 和原来存储的 Secret 一起用 Hash 函数计算,将所得结果与 ELC 中的第 1 部分比较,若两者相同,AA 向安装程序发送准许安装的消息.

(6) 安装程序解密收到的消息,并验证时间戳,证实与第(3)步发送的一致,即着手安装.

(7) 若第5步的比较不一致,则AA向安装程序发送夭折消息.

5.9.2 软件执行的验证

得到授权的客户在成功地安装了所购得的软件之后,要运行其已安装的可执行软件还需接受AA的验证,以防止非授权的用户运行.其过程如图7所示.



①客户计算机,②验证代理AA,③执行软件的请示,④验证线索,⑤安装,⑥执行线索.

Fig. 7 Secure execution procedure

图7 安全执行过程

(1) 当客户运行一个可执行文件时将生成两个线索并行运行,第1个线索执行该文件,第2个线索验证该客户的电子许可证.并行运行是为了提高效率,因为电子许可证的验证很费时.验证线索首先建立与AA的连接,发出执行软件的请求.

(2) AA使用商家的公钥解密ELC的第2部分,得到E_{PKC}(Product-Code,LicenseNo),并发给验证线索.

(3) 验证线索用客户私钥解密收到的消息,得到(Product-Code,LicenseNo).然后生成一个时间戳,将其与(Product-Code,LicenseNo)一起用对称密钥K加密,发给AA.

(4) AA收到后对其解密,并与ELC中的第2部分进行解密后加以比较.若两者相同,则验证成立;否则为非法用户,AA发送一个夭折消息给验证线索,后者使执行线索夭折.

对不同客户来说,其C-ID,Password和SKC都不相同,故防止非法拷贝软件的运行是安全的.本协议的不足之处是,验证代理AA常常驻客户计算机的内存,而且要求客户计算机的操作系统能保证AA的安全.

6 结束语

电子商务中的协议研究是电子商务研究的一个重要方面.正如上文所述,电子商务协议设计的重要原则首推安全性,没有安全就没有可被人们接受的电子商务.安全问题如今是信息社会和网络经济的一个极为关键的课题,有一支庞大的队伍在研究和开发,电子商务中的安全仅是它的一个方面.在本文例举的协议中,对称加密算法DES和非对称加密算法RSA是最为行之有效的方法,因而被广泛使用.信息的保密传送以及保证不可否认性的数字签名均有赖于RSA和DES.当然,新的加密算法层出不穷,这里不作深入讨论.

电子商务中协议的原子性是本文涉及的另一概念.本文介绍了Tygar引入的3种原子性以及它们在具体协议中的实践.是否还有其他类型的原子性,这仍然是一个要予以研究的课题.

匿名性是一个实际生活中需要的概念.人们对有关协议进行了卓有成效的研究,但在实用性及效率尚需做进一步的工作.

贸易代理在移动通信如日中天的今天显然具有宽广的应用前景.本文介绍的协议只是初步尝试,尚未涉及Agent和商家服务器的安全性,有关Agent Transfer Protocol(ATP)方面的内容亦未作介绍.这些有趣的课题均值得我们进一步研究.

References:

[1] Tygar, J. D. Atomicity versus anonymity: distributed transactions for electronic commerce, invited talks. In: Gupta, A., Shmueli, O., Widom, J., eds. Proceedings of the 24th Annual International Conference on Very Large Data Bases. New York: Morgan Kaufmann Publishers, 1998. 1~12.

[2] Dogac, A. Introduction, special section on electronic commerce. SIGMOD Record, 1998,27(4):5~6.

[3] Pernul, G., Madria, S. K. Preface. In: Bauknecht, K., Kumar, M. S., Pernul, G., eds. Proceedings of the 1st

International Conference on Electronic Commerce and Web Technology. London: Springer-Verlag, 2000.

[4] Meltzer, B., Glushko, R. XML and electronic commerce: enabling the network economy. SIGMOD Record, 1998,27(4):21~24.

[5] Bonifati, A., Ceri, S. Comparative analysis of five XML query languages. SIGMOD Record, 2000,29(1):68~79.

[6] Ives, Z. G., Lu, Y. XML query languages in practice: an evaluation. In: Lu, Hong-jun, Zhou, Ao-ying, eds. Proceedings of the 1st International Conference on Web-Age Information Management. Hong Kong: Springer-Verlag, 2000. 29~40.

[7] Chen, Q., Dayal, U., Hsu, M., *et al*. Dynamic-Agents, Workflow and XML for E-Commerce Automation. In: Bauknecht, K., Kumar, M. S., Pernul, G., eds. Proceedings of the 1st International Conference on Electronic Commerce and Web Technology. London: Springer-Verlag, 2000. 314~323.

[8] Anutariya, C., Wuwongse, V., Nantajeewarawat, E., *et al*. Towards a foundation for XML document databases. In: Bauknecht, K., Kumar, M. S., Pernul, G., eds. Proceedings of the 1st International Conference on Electronic Commerce and Web Technology. London: Springer-Verlag, 2000. 324~333.

[9] Günther, O., Ricou, O. An XML/XSL-based software architecture for application service providers. In: Bauknecht, K. Kumar, M. S., Pernul, G., eds. Proceedings of the 1st International Conference on Electronic Commerce and Web Technology. London: Springer-Verlag, 2000. 334~348.

[10] Garofalakis, M., Gionis, A., Rastogi, R., *et al*. XTRACT: a system for extracting document type descriptors from XML documents. SIGMOD Record, 2000,29(2):165~176.

[11] Chaum, D., Fiat, A., Naor, M. Untraceable electronic cash. In: Advances in Cryptology: Crypto'88 Proceeding. Berlin, Springer-Verlag, 1990. 200~212.

[12] Brickell, E., Gemmell, P., Kravitz, D. Trustee-Based tracing extensions to anonymous cash and the making of anonymous change. In: Proceedings of the 6th ACM-SIAM Symposium on Discrete Algorithms. 1995. 457~466.

[13] http://www.digicash.com.

[14] Cox, B. Maintaining privacy in electronic transactions. Technical Report, TR1994 8, Information Networking Institute, 1994.

[15] Cox, B., Tygar, J. D., Sirbu, M. Netbill security and transaction protocol. In: Proceedings of the 1st USENIX Workshop on Electronic Commerce. 1995. 77~88.

[16] http://www.netbill.com/.

[17] Domingo-Ferrer, J., Herrea-Joancomarti, J. An anonymous electronic commerce scheme with an off-line authority and untrusted agents. SIGMOD Record, 1998,27(4):62~67.

[18] Rivest, R., Shamir, A., Adleman, L. A method for obtaining digital sighatures and public-key cryptosystems. Coimmunications of the ACM, 1978,21(2):120~126.

[19] Gray, J. Notes on data base operating systems. In: Bayer, R., Graham, R. M., Seegmuller, eds. Operating Systems: an Advanced Course. Springer-Verlag, 1978.

[20] Gray, J., Reuter, A. Transactions Processing: Techniques and Concepts. San Fransisco: Morgan Kaufmann Publishers, 1994.

[21] Lynch, N., Merritt, M., Weihl, W., *et al*. Atomic Transaction. San Mateo, CA: Morgan Kaufmann Publishers, 1994.

[22] Tygar, J. D. Atomicity in electronic commerce. In: Proceedings of the 15th Annual ACM Symposium on Principles of Distributed Computing. 1996. 8~26.

[23] Camp, L., Sirbu, M., Tygar, J. D. Token and notational money in electronic commerce. In: Proceedings of the 1st USENIX Workshop on Electronic Commerce. 1995. 1~12.

[24] Sirbu, M., Tygar, J. D. Netbill: an internet commerce system optimized for network delivered services. IEEE Personal Communications, 1995,2(4):34~39.

[25] Franklin, M., Reiter, M. Fair exchange with a semi-trusted third party. In: Proceedings of the 4th ACM Conference on Computer and Communications Security. 1997. 1~5.

[26] Manasse, M. The millicent protocols for electronic commerce. In: Proceedings of the 1st USENIX Workshop on Electronic

Commerce. 1995. 117~123.

[27] Wu, Shi-zhong, Zhu, Shi-xiong, Zhang, Wen-zheng, *et al*, translated. Applied Cryptography: Protocols, Algorithms, and Source Code in C. 2nd ed, Beijing: Machine Industry Press, 2001 (in Chinese).

[28] Diffie, W., Hellman, M. New directions in cryptograph. IEEE Transactions on Information Theory, 1976,22:644~645.

[29] Visa USA and Anderson Consulting, 1992 Credit Card Functional Cost Study. 1992.

[30] Master Card, Inc., Visa, Inc. SET Draft Specification.

[31] Camp, L., Harkavy, M., Tygar, J. D., *et al*. Anonymous atomic transactions. In: Proceedings of the 2nd USENIX Workshop on Electronic Commerce. 1996. 123~133.

[32] Merwe, J., Von Solms, S. H. Electronic commerce with secure intelligent trade agents. In: Information and Communication Security. LNCS 1334, Springer-Verlag, 1997. 452~462.

[33] Berger, R., Peralta, R., Tedrick, T. A provably secure oblivious transfer protocol. In: Advances in Cryptology—EUROCRYPT'84. LNCS209, Springer Verlag, 1985. 408--416.

[34] Even, S., Golderich, O., Lempel, A. A randomizing protocol for signing contracts. Communications of the ACM, 1985, 28(6):637~647.

[35] Tedrick, T. Fair exchange of secrets. Advances in Cryptology—CRYPTO'84. LNCS 196, Springer-Verlag, 1985. 434~438.

[36] Software Piracy. http://www.nopiracy.com.

[37] Lee, Suny-min, Lee, Hyung-woo, Kim, Tai-yun. A secure electronic software distribution protocol based on PKC. In: Bauknecht, K., Kumar, M. S., Pernul, G., eds. Proceedings of the 1st International Conference on Electronic Commerce and Web Technologies. London Greenwich, 2000. 63~71.

附中文参考文献:

[27] 吴世中,祝世雄,张文政,等译.应用密码学:协议、算法与C源程序.第2版,北京:机械工业出版社,2001.

An Overview of Protocol Research in Electronic Commerce*

ZHOU Long-xiang

(Institute of Mathematics, Academy of Mathematics and System Sciences, The Chinese Academy of Sciences, Beijing 100080, *China)*

E-mail: lxzhou@math08.math.ac.cn

http://www.amss.ac.cn

Abstract: This is an overview of protocol research in electronic commerce. Electronic commerce protocols are the technical foundation to carry out the electronic commerce. The principles for designing electronic commerce protocols such as security, anonymity, atomicity, nonrepudiation and transaction size are introduced. Some famous existing electronic commerce protocols are described and analyzed as well.

Key words: electronic commerce; electronic commerce protocol; security; anonymity; atomicity; nonrepudiation; transaction size

* Received February 16, 2001; accepted May 21, 2001

Supported by the National Natural Science Foundation of China under Grant No. 69983011