兩岸資訊（信息）技術研討會

論文集

Proceedings of the Cross-Strait Information Technology Workshop

July 6 ~ 11, 1999, Taiwan

National Central University,

Taiwan

兩岸資訊（信息）技術研討會

論文集

Proceedings of the Cross-Strait Information Technology Workshop

July 6 ~ 11, 1999, Taiwan

National Central University,

Taiwan

誌 謝

特別感謝行政院大陸委員會以及立青文教基金會對於本次會議所提供的協助與指教。

兩岸資訊（信息）技術研討會

一九九九年七月

研討會主題

近年來，電腦網路技術急速進步，應用範圍幾乎深入所有社會活動。對人類生活、文化及思考方式，均有深遠影響。本研討會乃邀約兩岸學者專家，針對目前正熱烈發展中且對社會將產生立即而明顯衝擊的電腦網路應用技術，交換心得和經驗，期能共同為此項技術之提昇及應用而努力。

本研討會主題為「電腦網路的應用對社會之影響」，會中將徵求論文，並邀請兩岸學者專題演講：

- 電子商務
- 網路教學
- 電子圖書館

主辦單位：　中央大學

協辦單位：　東南大學

研討會地點：中央大學（臺灣，中壢）

會議時間：1999 年 7 月 6 日～11 日

籌備委員

研討會召集人：

劉兆漢(中央大學校長)

顧冠群(東南大學校長)

籌備委員：

劉寶鈞(中央大學)

余貴坤(中央大學)

黃興燦(中央大學)

范國清(中央大學)

曾黎明(中央大學)

許健平(中央大學)

許通安(中央大學)

薛義誠(中央大學)

曾煜棋(中央大學)

王能斌(東南大學)

沈再福(東南大學)

龔　儉(東南大學)

張月琳(東南大學)

史蘭新(東南大學)

羅軍舟(東南大學)

論文集

兩岸資訊（信息）技術研討會

目錄

Technical Session I : Electronic Commerce

Technical Session II : Distance Learning

Technical Session III : Information Technology and Miscellneous

Technical Session IV : Digital Library

附錄：

电子商务的安全技术

罗军舟

（东南大学计算机科学与工程系，中国南京 210096）

摘　要：保证数据传输的安全性和交易者身份的真实性是推广应用电子商务的关键问题。本文在分析了电子商务中的四个安全要素基础上，论述了电子商务使用的几种常用基本安全技术，包括加密、数字签名、电子证书、电子信封和双重签名，然后对公开密钥框架(PKI)、电子安全交易（SET）和防火墙等三种综合安全技术进行较详细介绍，并给出了作者正在研究开发的防火墙系统设计。

关键词：电子商务，安全技术，加密，数字签名，证书，认证，防火墙

一、引言

电子商务(Electronic Commerce, EC)就是利用电子数据交换(EDI)、电子邮件(E-mail)、电子资金转帐（EFT）及 Internet 的主要技术在个人间、企业间和国家间进行无纸化的业务信息的交换。据统计，1997 年企业间通过电子商务的交易额达 80 亿美元，估计到 2001 年将达到 3270 亿美元，其增长速度高达 4000%。可是，尽管电子商务的发展势头非常惊人，但它在全球贸易额中只占极小的一部分。一个主要的障碍就是如何保证传输数据的安全和交易对方的身份确认。因此，从传统的基于纸张的贸易方式向电子化的贸易方式转变的过程中，如何保持电子化的贸易方式与传统方式一样安全可靠，则是人们关注的焦点，同时也是电子商务全面应用的关键问题之一。

二、安全要素

1. 有效性

EC 以电子形式取代了纸张，那么如何保证这种电子形式的贸易信息的有效性则是开展 EC 的前提。EC 作为贸易的一种形式，其信息的有效性将直接关系到个人、企业或国家的经济利益和声誉。因此，要对网络故障、操作错误、应用程序错误、硬件故障、系统软件错误及计算机病毒所产生的潜在威胁加以控制和预防，以保证贸易数据在确定的时刻、确定的地点是有效的。

2. 机密性

EC 作为贸易的一种手段，其信息直接代表着个人、企业或国家的商业机密。传统的纸面贸易都是通过邮寄封装的信件或通过可靠的通信渠道发送商业报文来达到保守机密的目的。EC 是建立在一个开放的网络环境（如：Internet 网）上的，维护商业机密是 EC 全面推广应用的重要保障。因此，要预防非法的信息存取和信息在传输过程中被非法窃取。

3. 完整性

EC 简化了贸易过程，减少了人为的干预，同时也带来维护贸易各方商业信息的完整、

统一的问题。由于数据输入时的意外差错或欺诈行为，可能导致贸易各方信息的差异。此外，数据传输过程中信息的丢失、信息重复或信息传送的次序差异也会导致贸易各方信息的不同。贸易各方信息的完整性将影响到贸易各方的交易和经营策略，保持贸易各方信息的完整性是 EC 应用的基础。因此，要预防对信息的随意生成、修改和删除，同时要防止数据传送过程中信息的丢失和重复并保证信息传送次序的统一。

4. 可靠性

EC 可能直接关系到贸易双方的商业交易，如何确定要进行交易的贸易方正是进行交易所期望的贸易方，这一问题则是保证 EC 顺利进行的关键。在传统的纸面贸易中，贸易双方通过在交易合同、契约或贸易单据等书面文件上手写签名或印章来鉴别贸易伙伴，确定合同、契约、单据的可靠性并预防抵赖行为的发生。这也就是人们常说的“白纸黑字”。在无纸化的 EC 方式下，通过手写签名和印章进行贸易方的鉴别已是不可能的。因此，要在交易信息的传输过程中为参与交易的个人、企业或国家提供可靠的标识。

三、安全技术

为了满足电子商务的安全要求，EC 系统必须利用安全技术为 EC 活动参与者提供可靠的安全服务，主要包括：鉴别服务、访问控制服务、机密性服务、不可否认服务等。鉴别服务是对贸易方的身份进行鉴别，为身份的真实性提供保证；访问控制服务通过授权对使用资源的方式进行控制，防止非授权使用资源或控制资源，有助于贸易信息的机密性、完整性和可控性；机密性服务的目标为 EC 参与者信息在存储、处理和传输过程中提供机密性保证，防止信息被泄露给非授权信息获得者；不可否认服务针对合法用户的威胁，为交易的双方提供不可否认的证据，来解决因否认而产生的争议提供支持。

各种 EC 安全服务都是通过安全技术来实现的。EC 使用的主要安全技术包括：加密、数字签名、电子证书、电子信封和双重签名等。

1. 加密技术

加密技术是 EC 采取的基本安全措施，贸易方可根据需要在信息交换的阶段使用。加密技术分为两类，即对称加密和非对称加密。

在对称加密方法中，采用相同的加密算法并只交换共享的专用密钥（加密和解密都使用相同的密钥）。如果进行通信的贸易方能够确保专用密钥在密钥交换阶段未曾泄露，那么机密性和报文完整性就可以通过这种加密方法加密机密信息和通过随报文一起发送报文摘要或报文散列值来实现。因此，对称加密技术存在着在通信的贸易方之间确保密钥安全交换的问题。此外，对称加密方式无法鉴别贸易发起方或贸易最终方。数据加密标准（DES）由美国国家标准局提出，是目前广泛采用的对称加密算法，主要应用于银行业中的 EFT 领域。DES 的密钥长度为 56 位。

在非对称加密体系中，密钥被分解为一对，即公开密钥或专用密钥。公开密钥（加密密钥）通过非保密方式向他人公开，而专用密钥（解密密钥）加以保存。公开密钥用于对机密性的加密，专用密钥则用于对加密信息的解密。专用密钥只能由生成密钥对的贸易方掌握，公开密钥可广泛发布，但它只对应于生成该密钥的贸易方。贸易甲方生成一对密钥，公布公开密钥；贸易方乙得到该公开密钥，使用该密钥对机密信息进行加密，然后发送给贸易甲方；贸易甲方再用自己保存的专用密钥对加密后的信息进行解密。贸易方只能用其专用密钥解密由其公开密钥加密后的任何信息。RSA（Rivest, Shamir and Adleman）算法是

非对称加密领域内最为著名的算法 °

2. 数字签名

数字签名是非对称加密技术的一类应用 °它的主要方式是：报文发送方从报文文本中生成一个 128 位的散列值（或报文摘要），并用自己的专用密钥对这个散列值进行加密，形成发送方的数字签名；然后，这个数字签名将作为报文的附件和报文一起发送给报文的接收方；报文接收方首先从接收到的原始报文中计算出 128 位的散列值（或报文摘要），接着再用发送方的公开密钥来对报文附加的数字签名进行解密 °如果两个散列值相同，那么接收方就能确认该数字签名是发送方的 °通过数字签名能够实现对原始报文的鉴别和不可否认性 °

ISO/IEC JTC1 已经起草有关的国际标准规范 °该标准的题目是“信息技术安全技术带附件的数字签名方案”，它由概述和基于身份的机制两部分构成 °

3. 电子证书

数字签名是基于非对称加密技术的，存在两个明显的问题：第一，如何保证公开密钥的持有者是真实的；第二，大规模网络环境下公开密钥的产生 `分发和管理 °由此，证书签发机构（Certificate Authority, CA）应运而生，它是提供身份验证的第三方机构，由一个或多个用户信任的组织实体构成 °CA 核实某个用户的真实身份以后，签发一份报文给该用户，以此作为网上证明自己身份的依据 °这个报文称为电子证书，包括：唯一标识证书所有者（即贸易方）的名称 `唯一标识证书签发者的名称 `证书所有者的公开密钥 `证书签发者的数字签名 `证书的有效期及证书的序列号等 °电子证书能够起到标识贸易方的作用，是目前 EC 广泛采用的技术之一 °常用的证书有：持卡人证书 `商家证书 `支付网关证书 `银行证书和发卡机构证书等 °微软公司的 Internet Explorer 和网景公司的 Navigator 都提供了电子证书的功能作为身份鉴别的手段 °

4. 电子信封

电子信封是为了解决传送更换密钥问题而产生的技术，它结合了对称加密和非对称加密技术的各自优点 °发送者使用随机产生的对称密钥加密数据，然后将生成的密文和密钥本身一起用接收者的公开密钥加密（称为电子信封）并发送；接收者先用自己的专用密钥解密电子信封，得到对称密钥，然后使用对称密钥解密数据 °这样，保证每次传送数据都可有发送方选定不同的对称密钥 °

5. 双重签名

在实际商务活动中经常出现这种情形，即持卡人给商家发送订购信息和自己的付款帐户信息，但他/她不愿让商家看到自己的付款帐户信息，也不愿让处理商家付款信息的第三方看到定货信息 °在 EC 中要能做到这点，需使用双重签名技术 °持卡人将发给商家的信息（报文 1）和发给第三方的信息（报文 2）分别生成报文摘要 1 和报文摘要 2，合在一起生成报文摘要 3，并签名；然后，将报文 1 `报文摘要 2 和报文摘要 3 发送给商家，将报文 2 `报文摘要 1 和报文摘要 3 发送给第三方；接收者根据收到的报文生成报文摘要，再与收到的报文摘要合在一起，比较结合后的报文摘要和收到的报文摘要 3，确定持卡人的身份和信息是非被修改过 °双重签名解决了三方参加电子贸易过程中的安全通信问题 °

四 ` 公开密钥框架（PKI）

与 DNS 和 X.500 类似，公开密钥框架（Public Key Infrastructure, PKI）也是一种网络基础设施，其目标是向网络用户和应用程序提供公开密钥的管理服务。为了使用户在不可靠的网络环境中获得真实的公开密钥，PKI 引入公认可信的第三方；同时避免在线查询集中存放的公开密钥产生的性能瓶颈，PKI 引入电子证书。可信的第三方是 PKI 的核心部件，正是由于它的中继，系统中任意两个实体才能建立安全联系。

电子证书中第三方的数字签名，使用户可以离线地确认一个公开密钥的真实性。当证书中认可的事实发生变化时，证书发布者必须使用某种机制来撤销以前发出、但现在失效的证书。除了证书的有效期外，证书撤销列表（CRL）是另一种证书有效期控制机制。证书发布者定期发布 CRL，列出所有曾发布但当前已被撤销的证书号，证书的使用者依据 CRL 即可验证某证书是否已被撤销。

1. PKI 结构模型

PKI 框架有三类实体：管理实体、端实体和证书库。管理实体是 PKI 的核心，是 PKI 服务的提供者；端实体是 PKI 的用户，是 PKI 服务的使用者；证书库是一个分布式数据库，用于证书/CRL 存放和检索。

证书签发机构（CA）和注册机构（RA）是两种管理实体。CA 是 PKI 框架中唯一能够发布/撤销证书的实体，维护证书的生命周期；RA 负责处理用户请求，在验证了请求的有效性后，代替用户向 CA 提交。RA 可以单独实现，也可以合并在 CA 中实现。作为管理实体，CA/RA 以证书方式向端实体提供公开密钥的分发服务。

持有者和验证者是两种端实体。持有者是证书的拥有者，是证书所声明事实的主体。持有者向管理实体申请并获得证书，也可以在需要时请求撤销或更新证书。持有者使用证书鉴别自己的身份，从而获得相应的权力。验证者通常是授权方，确认持有者所提供的证书的有效性和对方是否为该证书的真正拥有者，只有在成功鉴别之后才可授权对方。

证书库可有 WEB、FTP 或 X.500 目录来实现。由于证书库中存取对象是证书和 CRL，其完整性由数字签名保证，因此对证书库的操作可在无特殊安全保护的信道上传输。

不同的实体间通过 PKI 操作完成证书的请求、确认、发布、撤销、更新和获取等过程。PKI 操作分成存取操作和管理操作两类。前者涉及管理实体/端实体与证书库之间的交互，操作的目的是向/从证书库存放/读取证书和 CRL，后者涉及管理实体与端实体之间或管理实体内部的交互，操作的目的是完成证书的各项管理任务和建立证书链。

2. PKI 层次模型

PKI 框架描述为三个层次。最低层是传输层，向上提供 PKI 操作报文的可靠传输，可以是运输层协议（如：TCP），或应用层协议（如：HTTP、SMTP、FTP）。中间层是密码学服务层，向上提供加解密、数字签名和报文摘要等基本密码学服务，可由 RSA、MD 5 和智能卡接口等模块实现。最高层是证书服务层，使用下两层提供的加密和传输服务，向用户提供证书的请求、签证、发布、撤销和更新等服务。

PKI 的三类实体使用了三层服务。证书库无需特殊的安全交互措施，所以仅使用传输层服务分发证书和 CRL；管理实体和端实体使用证书服务层构造 PKI 证书操作报文，使用密码学服务层作鉴别和保护交互信息，使用传输层服务传送报文。

3. X.509 证书

ISO/ITU、ANSI、IETF 等组织制定的标准 X.509，对电子证书进行了定义，对 X.509 证书和 CRL 做了标准化工作，不同组织定义的证书格式并不完全相同。X.509 证书适用于大规模网络环境，它的灵活性和扩展性能够满足各种应用系统不同类型的安全要求。

X.509 证书具有如下五个方面的特性 °第一，支持多种算法 °X.509 证书独立于算法，CA 根据需要选择证书的签名和摘要算法，以及端实体所拥有密钥对的类型 °摘要算法有 MD2 `MD5 和 SHA-1，证书签名算法有 RSA 和 DSA，密钥对类型有 RSA 密钥 `DSA 签名密钥 `D-H 密钥交换密钥 `KEA 密钥和 ECDSA 密钥；第二，支持多种命名机制 °X.509 证书除了使用 X.500 名字机制标识持证者和验证者，还支持 Email 地址 `IP 地址 `DNS 名和 URI °第三，限制证书（公开密钥）的用途 °CA 能够规定证书的使用范围，如：签名 ` 不可否认 `密钥加密 `数据加密 `密钥协商 `证书签发和 CRL 签发等 °第四，定义证书遵循的策略 °每个 CA 都定义了一定的安全策略，规范证书的操作过程 °这些策略包括：CA 的命名空间 `身份验证 `撤销机制 `法律责任和收费等 °第五，控制信任关系的传递 °建立 CA 体系，跨域认证，使得每个 CA 除负责本域的证书管理任务外，还要维护与其他 CA 间的信任关系 °X.509 证书定义若干字段用于控制信任关系的传递，CA 能够将自己管理域的安全策略体现在信任关系中 °

五 ` 安全电子交易（SET）

安全电子交易（Secure Electronic Transaction, SET）是一个通过开放网络（包括 Internet 网络）进行安全资金支付的技术标准，由 Visa 和 MasterCard 组织共同制定，1997 年 5 月联合推出 °由于它得到了 IBM `HP `Microsoft `Netscape `VeriFone `GTE `Terisa 和 VeriSign 等很多大公司的支持，它已成为事实上的工业标准，目前它已获得 IETF 标准的认可 °

SET 向基于信用卡进行电子化交易的应用提供了实现安全措施的规则 °SET 主要由 3 个文件组成，分别是 SET 业务描述 `SET 程序员指南和 SET 协议描述 °SET 规范涉及的范围：(1) 加密算法的应用（例如 RSA 和 DES）；(2) 证书信息和对象格式；(3) 购买信息和对象格式；(4) 确认信息和对象格式；(5) 划帐信息和对象格式；(6) 对话实体之间消息的传输协议 °SET 1.0 版已经公布并可应用于任何银行支付服务 °

SET 主要目标如下:

(1) 信息在 Internet 上安全传输，保证网上传输的数据不被黑客窃取；

(2) 定单信息和个人帐号信息的隔离，当包含持卡人帐号信息的定单送到商家时，商家只能看到定货信息，而看不到持卡人的帐户信息；

(3) 持卡人和商家相互认证，以确定通信双方的身份 °一般由第三方机构负责为在线通信双方提供信用担；

(4) 要求软件遵循相同协议和报文格式，使不同厂家开发的软件具有兼容和互操作功能，并且可以运行在不同的硬件和操作系统平台上 °

1. SET 的购物流程

电子商务的工作流程与实际的购物流程非常接近，使得电子商务与传统商务可以很容易融合，用户使用也没有什么障碍 °从顾客通过浏览器进入在线商店开始，一直到所定货物送货上门或所定服务完成，然后帐户上的资金转移，所有这些都是通过公共网络(Internet)完成的 °如何保证网上传输数据的安全和交易对方的身份确认是电子商务能否得到推广的关键 °这正是 SET 所要解决的最主要的问题 °从一个完整的购物处理流程看 SET 的工作过程，如图 1 所示 °

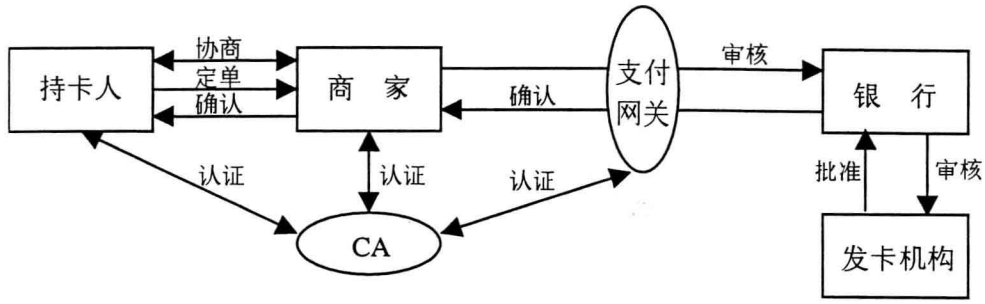

图 1 SET 的工作过程

(1)持卡人使用浏览器在商家的 WEB 主页上查看在线商品目录，浏览商品 。

(2)持卡人选择要购买的商品 。

(3)持卡人填写定单，包括项目列表 、价格 、总价 、运费 、搬运费 、税费 。定单可通过电子化方式从商家传过来，或由持卡人的电子购物软件建立 。有些在线商场可以让持卡人与商家协商物品的价格（例如出示自己是老客户的证明，或给出竞争对手的价格信息）。

(4)持卡人选择付款方式，此时 SET 开始介入 。

(5)持卡人发送给商家一个完整的定单及要求付款的指令 。在 SET 中，定单和付款指令由持卡人进行数字签名，同时利用双重签名技术保证商家看不到持卡人的帐号信息 。

(6)商家收到定单后，向持卡人的金融机构请求支付认可 。通过支付网关到银行，再到发卡机构确认，批准交易 。然后返回确认信息给商家 。

(7)商家发送定单确认信息给顾客 。顾客端软件可记录交易日志，以备将来查询 。

(8)商家给顾客装运货物，或完成订购的服务 。到此为止，一个购买过程已经结束 。商家可以立即请求银行将钱从购物者的帐号转移到商家帐号，也可以等到某一时间，请求成批划帐处理 。

(9)商家从持卡人的金融机构请求支付 。在认证操作和支付操作中间一般会有一个时间间隔，例如在每天的下班前请求银行结一天的帐 。

前三步与 SET 无关，从第四步开始 SET 起作用，一直到第九步，在处理过程中，通信协议 、请求信息的格式 、数据类型的定义等，SET 都有明确的规定 。在操作的每一步，持卡人 、商家和支付网关都通过 CA 来验证通信主体的身份，以确保通信的对方不是冒名顶替 。

2. SET 的认证

(1) 证书

SET 中主要的证书是持卡人证书和商家证书 。

持卡人证书：它是支付卡的一种电子化的表示 。持卡人证书不包括帐号和终止日期信息，而是用单向哈希算法根据帐号和截止日期生成的一个码，如果知道帐号 、截止日期 、密码值即可导出这个码值，反之不行 。

商家证书：它就像是贴在商家收款台小窗上的付款卡贴画，以表示它可以用什么卡来结算 。在 SET 环境中，一个商家至少应有一对证书，与一个银行打交道；一个商家也可以有多对证书，表示它与多个银行有合作关系，可以接受多种付款方法 。

除了持卡人证书和商家证书以外，还有支付网关证书 、银行证书 、发卡机构证书 。

(2) CA

持卡人可从公开媒体上获得商家的公开密钥，但持卡人无法确定商家不是冒充的（有信誉），于是持卡人请求 CA 对商家认证 。CA 对商家进行调查 、验证和鉴别后，将包含商

家公开密钥的证书经过数字签名，传给持卡人 °同样，商家也可对持卡人进行验证 °

CA 的主要功能包括：接收注册请求，处理 `批准/拒绝请求，颁发证书 °

在实际运作中，CA 也可由大家都信任的一方担当，例如在客户 `商家 `银行三角关系中，客户使用的是由某个银行发的卡，而商家又与此银行有业务关系(有帐号) °在此情况下，客户和商家都信任该银行，可由该银行担当 CA 角色，接收 `处理卡客户证书和商家证书的验证请求 °又例如，对商家自己发行的购物卡，则可由商家自己担当 CA 角色 °

(3) 证书的树形验证结构

在双方通信时，通过出示由某个 CA 签发的证书来证明自己的身份，如果对签发证书的 CA 本身不信任，则可验证 CA 的身份，依次类推，一直到公认的权威 CA 处，就可确信证书的有效性 °每一个证书与签发证书的实体的签名证书关联 °SET 证书正是通过信任层次来逐级验证的 °例如，C 的证书是由 B 的 CA 签发的，而 B 的证书又是由 A 的 CA 签发的，A 是权威的机构，通常称为根 CA °验证到了根 CA 处，就可确信 C 的证书是合法的 °

在网上购物实现中，持卡人的证书与发卡机构的证书关联，而发卡机构证书通过不同品牌卡的证书连接到根 CA，而根的公开密钥对所有的 SET 软件都是已知的，可以校验每一个证书 °

六 ` 防火墙技术

网络防火墙技术是一种用来加强网络之间访问控制和防止外部网络用户以非法手段通过外部网络进入内部网络 `访问内部网络资源 `保护内部网络操作环境的特殊网络互连设备 °它对两个或多个网络之间传输的数据包，按照一定的安全策略来实施检查，决定网络之间通信的权限，并监视网络的运行状态 °防火墙系统的实现技术主要分为分组过滤(Packet Filter）和代理服务（Proxy Service）两种 °

分组过滤技术是一种基于路由器的技术，由分组过滤路由器对IP分组进行选择，允许或拒绝特定的分组通过 °过滤一般是基于一个IP分组的有关域（IP源地址 `IP目的地址 `TCP/UDP源端口或服务类型和TCP/UDP目的端口或服务类型）进行的 °基于IP源/目的地址的过滤，即根据特定组织机构的网络安全规则，过滤掉具有特定IP地址的分组，从而保护内部网络；基于TCP/UDP源/目的端口的过滤，因为端口号区分了不同的服务类型或连接类型（如SMTP使用端口25，Telnet使用端口23等），所以为分组过滤提供了更大的灵活性 °通过防火墙系统中分组过滤路由器对特定端口IP分组的禁止，可以防止黑客利用不安全的服务对内部网络进行攻击 °

代理服务技术是由一个高层的应用网关作为代理服务器，接受外来的应用连接请求，进行安全检查后，再与被保护的网络应用服务器连接，使得外部服务用户可以在受控制的前提下使用内部网络的服务 °同样，内部网络到外部的服务连接也可以受到监控 °应用网关的代理服务实体将对所有通过它的连接作出日志记录，以便对安全漏洞的检查和收集相关的信息 °使用应用网关的高层代理服务实体有以下的优点：①隐蔽信息，内部受保护子网的主机名称等信息不为外部所知；②日志记录，便于网络安全管理；③可以由应用网关代理有关RPC的服务，进行安全控制 °

目前，比较完善的防火墙系统通常结合使用两种技术 °代理服务可以大大降低分组过滤规则的复杂度，是分组过滤技术的重要补充 °这儿介绍一种基于网络地址转换（Network Address Translator, NAT）的复合型防火墙系统，由我们自行研究和开发 °

1. 总体思想

代理技术造成性能下降的主要原因在于其在指定的应用服务中，传输的每一个报文都需代理主机转发，应用层的处理量过于繁重，改变这一状况的最理想的方案是让应用层仅处理用户身份鉴别的工作，而网络报文的转发由 TCP 层或 IP 层来完成。另一方面，包过滤技术仅仅是根据 IP 包中源及目的地址来判定一个包是否可以通过，而这两个地址是很容易被篡改和伪造的，一旦网络的结构暴露给外界后，就很难抵御 IP 层的攻击行为。

集中访问控制技术是在服务请求时由网关负责鉴别，一旦鉴别成功，其后的报文交互都直接通过 TCP/IP 层的过滤规则，无需象应用层代理那样逐个报文转发，这就实现了与代理方式同样的安全水平而处理量大幅下降，性能随即得到大大提高。另一方面，NAT 技术通过在网关上对进出 IP 包源与目的地址的转换，实现过滤规则的动态化。这样，由于 IP 层将内部网与外部网隔离开，使得内部网的拓扑结构、域名以及地址信息对外成为不可见或不确定信息，从而保证了内部网中主机的隐蔽性，使绝大多数攻击性的试探失去所需的网络条件。

2. 系统设计

图 2 给出了本防火墙系统的总体结构模型，由五大模块组成。

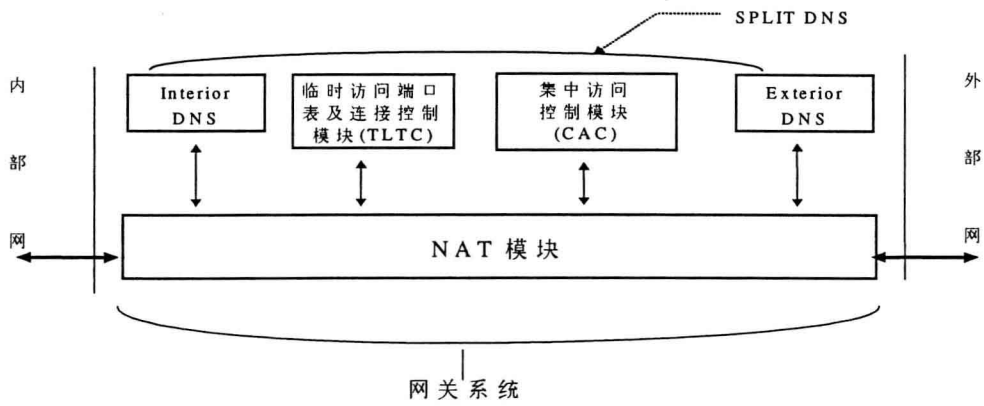

图 2　系统总体结构模型

NAT 模块依据一定的规则，对所有出入的数据包进行源与目的地址识别，并将由内向外的数据包中源地址替换成一个真实地址，而将由外向内的数据包中的目的地址替换成相应的虚拟地址。

集中访问控制（CAC）模块负责响应所有指定的由外向内的服务访问，并实施安全的鉴别，为合法用户建立相应的连接，并将这一连接的相关信息传递给 NAT 模块，保证在后续的报文传输时直接转发而无需控制模块干预。

临时访问端口表及连接控制（TLTC）模块通过监视外向型连接的端口数据动态维护一张临时端口表，记录所有由内向外的连接的源与目的端口信息，根据此表及预先配置好的协议集由连接控制模块决定哪些连接是允许的而哪些是不允许的，即根据所制定的规则（安全政策）禁止相应的由外向内发起的连接，以防止攻击者利用网关允许的由内向外的访问协议类型做反向的连接访问。由于本模块所实现的功能实际上仍属于 IP 包过滤的范畴，因此，它有可能与 NAT 模块所设定的过滤规则相冲突。基于这一原因，在系统总体设计中，本模块属于可选部分，将在实际操作时根据需要来安装或激活。

Interior DNS 和 Exterior DNS 分别为 NAT 模块机能所需的 Split-DNS 系统中的内部域名服务器和外部域名服务器（DNS），是 NAT 网关不可缺少的辅助部分。Split-DNS 系统的主要目的在于解决由于 NAT 模块对内外部网的地址屏蔽所造成的内外部域名解析不一致的

问题。内部网的域名解析由 Interior DNS 负责，外部网针对内部网的域名解析由 Exterior DNS 负责，两者间的数据同步通过内部通信机制完成。

3. 模块功能

- NAT 模块

NAT 模块是本系统核心部分，而且只有本模块与网络层有关，因此，这一部分应和 Unix 系统本身的网络层处理部分紧密结合在一起，或对其直接进行修改。本模块进一步可细分为包交换子模块、数据包头替换子模块、规则处理子模块、连接记录子模块与真实地址分配子模块及传输层过滤子模块。

- CAC 模块

集中访问控制模块可进一步细分为用户鉴别子模块和连接中继子模块及用户数据库。用户鉴别子模块主要负责与客户通过一种可信的安全机制交换各种身份鉴别信息，根据内部的用户数据库，识别出合法的用户，并根据用户预先被赋予的权限决定后续的连接形式。

连接中继子模块的主要功能是为用户建立起一条最终的无中继的连接通道，并在需要的情况下向内部服务器传送鉴别过的用户身份信息，以完成相关服务协议中所需的鉴别流程。

- SPLIT DNS 系统

内部、外部 DNS 模块可以利用现有的 DNS 服务程序，如 BIND（Berkley Internet Name Domain）软件包，通过与 NAT 模块不断交互，维持域名与地址对应关系的同步，维护两个动态的内部 DNS 数据库和外部 DNS 数据库来实现，既达到了总体的设计目标，又保持了对其他服务的透明性。

七、结束语

随着电子商务的发展，安全问题更加重要和更加突出。解决好这个问题，必须由安全技术和标准作保障。安全是一个“相对的”词汇，电子商务不断促使对安全技术进行探索研究和开发应用，获得一个安全的电子商务环境。本文介绍的安全技术和标准规范是 EC 应用中主要涉及的技术，还有一些安全技术及标准规范尚未列出。要保证 EC 安全可靠，首先要明确 EC 的安全隐患、安全等级和采用安全措施的代价，再选择相应的安全措施。EC 应用的安全方案已逐步形成，EC 时代即将到来。

参考文献

[1] 沈鸿，电子商务一基础篇，电子工业出版社，1998 年 9 月

[2] 国外评测，电子商务（EC）的安全要素及其相关技术，计算机世界，1997 年 29 期

[3] 丁燕舞，Internet 商务的安全认证，计算机世界，1997 年 46 期

[4] 罗军舟，王晖，顾冠群，混合型防火墙系统的实现，第九届全国数据通信学术会议，重庆，1998 年 9 月

[5] 罗军舟，顾冠群，EDI 中的数字签名技术，数据通信，1994 年第 3 期

[6] IETF PKIX WG, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, draft-ietf-pkix-ipki-part1-08.txt, June 1998