

基于三元对等鉴别的一体化网络接入机制研究

王海清, 苏伟, 董平

(北京交通大学 电子信息工程学院, 北京 100044)

摘要:网络安全接入机制在一体化网络完善过程中具有举足轻重的地位,目前通用的二元鉴别机制缺乏对执行端的验证,在某种程度上影响了网络安全性。为了保证网络安全,实现终端安全可信地接入核心网络,文中提出了一种基于三元对等鉴别的一体化网络安全接入机制。该鉴别认证机制能实现接入终端与接入交换路由器的双向身份鉴别,可以有效防止非授权终端接入网络,同时防止恶意接入交换路由器对终端的欺骗,即实现了终端、交换路由器和认证中心三个认证实体间的相互鉴别认证,并从性能和安全性等方面分析了此机制的优越性。文中提出的方法增强了一体化网络中对终端接入访问的安全控制,推动了三元对等鉴别技术的应用,促进了一体化网络的完善。

关键词:三元对等鉴别;一体化网络;双向身份鉴别;RSA

中图分类号:TP31

文献标识码:A

文章编号:1673-629X(2016)04-0096-05

doi:10.3969/j.issn.1673-629X.2016.04.021

Research on Identity Authentication Scheme in Universal Network Based on Tri-element Peer Authentication Method

WANG Hai-qing, SU Wei, DONG Ping

(School of Electronics and Information Engineering, Beijing Jiaotong University,
Beijing 100044, China)

Abstract: Identity authentication scheme in universal network is extremely important. General two-element peer authentication has shortcomings that it doesn't authenticate the router, which is a potential security problem. In order to guarantee the network security and realize terminal access to core network safely and credibly, a kind of integrated network security access mechanism based on tri-element peer authentication is put forward. In the new mechanism, terminal and router can authenticate each other by this way and effectively prevent unauthorized terminal access to networks, at the same time prevention of malicious access to exchange router for cheating terminal, which implements mutual identification authentication for terminal, exchange routers and certification center. The superiority of this mechanism is analyzed from performance and security and other aspects. The proposed method enhances the network security control of terminal access, promoting the application for ternary peer identification technology, raising the improvement of the integration of network.

Key words: tri-element peer authentication; universal network; two-way authentication; RSA

0 引言

一体化网络是一种新型互联网体系结构,其核心思想是通过引入接入标识、交换路由标识以及接入标识与交换路由标识之间的分离映射机制来支持身份与位置分离^[1]。一体化网络的身份与位置分离理念为当前盛行的基于 TCP/IP 网络在移动性、安全性和路由可扩展性上的问题提供了良好的解决思路。一体化网络将 IP 地址的双重属性分离,使节点的位置信息更为隐蔽,保护了用户的隐私性^[2]。用户不能了解到网络

的拓扑结构,因此可以缓解当前互联网中常见的中间人攻击(MITM)^[3]、分布式拒绝服务攻击(DDOS)^[4]以及权限提升攻击等。同传统互联网一样,网络安全对于一体化网络十分重要,必须设置安全认证机制保障外部终端在接入网络、切换接入域过程中的安全。

目前,关于一体化网络的研究资料越来越丰富,针对一体化网络的安全接入认证协议也取得了一些研究成果,例如:文献[5]中的身份标识和挑战应答组合的认证机制,文献[6]中身份标签和离散对数谜题组合

收稿日期:2015-07-22

修回日期:2015-10-26

网络出版时间:2016-03-22

基金项目:中央高校基本科研业务费专项资金(2014JBM004);北京高等学校青年英才计划项目(YETP0534)

作者简介:王海清(1990-),女,硕士研究生,研究方向为下一代互联网;苏伟,副教授,研究方向为信息网络、网络安全;董平,副教授,研究方向为信息网络、网络安全。

网络出版地址: <http://www.cnki.net/kcms/detail/61.1450.TP.20160322.1522.094.html>

的认证机制,文献[7]中利用随机数来验证身份的机制。如何建立更安全、可靠的新型网络体系成为一体化网络研究的重点。

文中在一体化网络体系结构的基础上,着重分析了一体化网络中的终端安全接入,同时结合我国自主知识产权的三元对等鉴别架构,推出了一种一体化网络终端的安全接入机制,并采用对称加密算法的数字签名方案来确保数据的机密性与完整性。

1 一体化网络的体系结构

一体化标识网络^[1]将网络划分为接入网与骨干网两部分。接入网由接入交换路由器和终端设备构成,主要作用是实现各类终端的安全接入;骨干网由接入交换路由器、核心路由器以及各种服务器(认证服务器、映射服务器等),通过接入交换路由器连接各个接入网。

一体化标识网络的创新点在于身份信息和位置信息的分离。接入网中使用身份标识来表示接入终端的身份信息;核心网中使用路由标识来表示路由信息。在接入网与核心网之间的接入交换路由器上实现接入标识和路由标识的替换。身份、位置信息分离的优势在于^[2]:

(1)用户的隐私性和安全性:克服了IP地址的双重属性,在身份与位置分离网络中,节点的身份标识与路由标识不能直接通信,即表示节点身份的身份标识不能在核心网中使用,核心网中的攻击者不能通过截获的数据包来分析身份信息,表示节点位置的路由标识不能在接入网中使用,在接入网中不能获取节点位置信息。

(2)路由可扩展性:在IPv4、IPv6发展过程中,由于IP地址分配不合理增加了路由表的聚合难度,导致路由表条目增长迅速。同时由于移动IP的发展,更加剧了核心路由的压力。身份与位置分离网络中,接入网中的移动IP等动态行为不会影响核心路由,从而避免了上述路由条目增加的压力,提高了核心路由的转发速度。

(3)移动性:移动IPv4^[8]、IPv6^[9]解决了传统互联网中的节点移动问题,但是存在显著的三角路由、移动切换时延长等问题。在身份与位置分离网络中,当节点移动到其他的网域中,由于节点的身份标识不会发生改变,只需要重新发布身份标识和路由标识的映射关系,简洁且高效。

一体化标识网络拥有良好的发展前景,但是网络安全威胁时刻存在,尤其是针对接入网中中断节点接入的安全认证。

因此探索更优质的安全认证机制,对于实现可靠

通信、保障网络安全至关重要。

2 三元对等鉴别原理

2.1 二元身份认证

在现有的终端实体的可信入网与控制中,最典型的方案有思科的网络准入控制技术(Network Admission Control, NAC),微软的网络访问保护技术(Network Access Protection, NAP),华为的端点准入防御技术(Endpoint Admission Defense, EAD)等。这些技术本质上都是采用一个通用的终端节点接入控制模型,如图1所示。

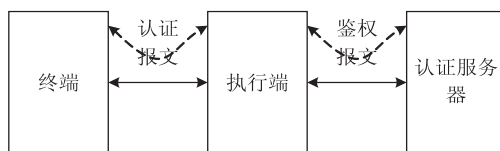


图1 二元身份认证模型

图1的认证模型包括三个元素:终端、执行端和认证服务器。执行端通常是与终端直连的网络设备,如路由器、交换机等。认证服务器扮演认证者的角色,在未通过认证服务器认证之前,终端与网络只能交互底层报文,在通过认证服务器的验证之后,终端才能与网络中其他设备交互上层报文。而执行端只是完成认证报文在终端和认证服务器之间的解封装、转发与封装以及根据端口是否处于认证状态对报文进行访问控制。在图1的认证模型中,真正参与认证的只有终端和认证服务器,因此被称为“二元身份认证模型”。

在二元身份认证模型中,由于没有验证执行端的可信性,攻击者很容易伪装成执行端对网络进行攻击,威胁网络安全;同时所有的认证报文都要经过认证服务器的处理,认证服务器负载随着网络规模的扩大而增加,这导致认证服务器很容易成为系统的瓶颈。因此,引入新型认证模型很有必要。

2.2 三元对等鉴别认证

三元对等鉴别(TePA)是西电捷通自主提出的一种信息安全领域普适性实体鉴别方案。此方案中提出的五次传递和调用可信第三方的机制,适用于实体间的双向身份鉴别^[10],能够满足“合法终端设备访问合法网络”的网络安全需求。

在TePA鉴别机制中,包括三个实体元素(A, B, C),实体C对于实体A、B来讲是完全可信的,A和B对于C来说是对等鉴别实体。此鉴别机制要求A和B通过同时拥有A、B公钥的可信第三方C来验证对方的公钥^[11]。

鉴别机制依赖在三个实体之间进行的五次认证信息交互,达成鉴别目的。图2为由B发起的鉴别机制,由A发起的鉴别机制原理相同^[12]。

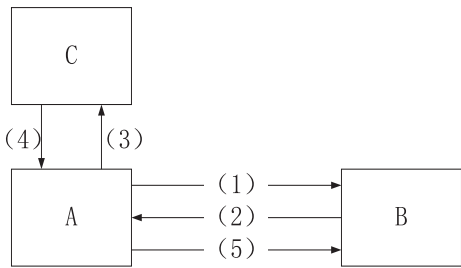


图 2 鉴别机制结构

鉴别过程如下：

- (1) A→B: A 发送随机数和身份信息、可选文本到 B;
- (2) B→A: B 发送随机数和身份信息、可选文本到 A;
- (3) A→C: A 发送 A、B 的身份信息及其他信息给 C,请求验证;
- (4) C→A: C 将对 A 和 B 的验证结果发送给 A;
- (5) A→B: A 将 C 对 A 的验证结果发送给 B。

2.3 基于三元对等鉴别的一体化网络接入机制

一体化网络结构的划分不同于传统互联网,从概念上讲,可以分为服务层和网通层。服务层主要负责业务的回话、控制和管理^[1],对应于传统互联网 IOS 的传输层;网通层主要负责下层通信,相当于 IOS 的网络层及以下的部分。

目前流行的认证方式包括:Web 认证、PPPoE 认证和 802.1x 认证。其中:Web 认证是利用 HTTP 协议传递认证消息,属于应用层认证;PPPoE 利用 PPP 链路协议在以太网上传递认证消息,属于链路层认证;802.1x 是利用 EAPOL 帧封装 EAP 认证协议,也属于链路层认证。不同认证方式优劣对比如图 3 所示。其中,链路层以 802.1x 为例,应用层以 Web 认证为例。

| | 链路层 (802.1x) | 网络层 | 应用层 (Web认证) |
|----|--|--------------------------------------|---|
| 优势 | 纯以太网技术内核,保持了IP网络无连接特性;网络综合造价成本低 | 屏蔽二层接入技术的差异,从而适应各种接入网络,同时有利于支持终端的移动性 | 不需要特殊的客户端软件,与系统平台无关,使用DHCP得到IP地址,没有额外的开销,并支持多播协议性 |
| 劣势 | 需要特定客户端软件 802.1x协议是一个2层协议,只负责完成对用户端口的认证控制,对于完成端口认证后,用户进入三层IP网络后,需要继续解决IP地址分配、三层网络安全等问题 | 在移动环境中的认证延时问题;在切换中的安全问题 | 用户的连接性差,不易检测到用户离线,不适合移动用户完成切换;在未认证前分配IP,造成资源浪费 |

图 3 不同认证方式对比

从图 3 的对比分析中可以看出:Web 认证开销小但是连接不稳定,同时不适合移动用户;链路层认证由于是直接承接在链路层数据帧上,二层接入技术的差异使这种直接面向二层的接入认证方式不能适用于不同的接入网络以及相互之间的切换^[13]。

基于以上分析,文中综合考虑一体化标识网络中

的安全和移动性问题,提出利用三元对等鉴别在网络层的安全接入机制。

在该机制中,认证中心 AS 是认证服务的关键,因为 AS 是整个认证系统中都信任的一个实体,是终端 Node 和接入交换路由器 ASR 交互信任信息的基础。作为网关,ASR 将接入网与核心网隔离开来,因此,为了保障核心网络的安全,ASR 身份可信性必须保证。在单向鉴别 Node 可信性之外,利用三元对等鉴别方法,也核实了 ASR 的可信性,保障了一体化标识网络的安全接入。

作为三元对等鉴别认证应用在通信领域的一个实例,WAPI 协议采用了基于数字证书的安全接入机制。数字证书是一种数字身份证,是经过证书授权中心数字签名的,包含公共密钥拥有者信息以及公开密钥的可信文件。采用数字证书的鉴别机制安全性比较高,但是,利用数字证书的认证机制对系统资源要求较高,因此,文中采用基于身份标识的安全接入认证机制。

3 安全接入机制

3.1 认证中的加密算法

根据密钥算法的不同,可以将加密算法分为两种:

(1) 对称加密算法。

通信双方使用相同的密钥进行加、解密。此密钥在通信开始之前由安全部门分配或者通信双方协商得到。常见的对称加密算法有 DES、3DES、AES 等块加密算法以及 RC4、SEAL 等流加密算法。

(2) 非对称加密算法。

通信双方使用不同的密钥进行加、解密。每个通信实体有一对密钥,一个称为公钥,是公开的,一个称为私钥,是只有自己知道的。当发送者 A 发送一条加密信息给接收者 B,为了保证只有 B 能破解此信息,使用 A 的公钥加密信息,当 B 收到加密信息后使用自己的私钥解密信息。这样就保证了信息的秘密性。除了加密信息之外,发送者 A 还可以利用自己的私钥对信息进行签名,当接收者 B 收到签名信息后,利用 A 的公钥解密,根据解密结果就能判断该信息是否来自发送者 A。常见的非对称加密算法有 RSA 和 ECC。

通过以上对比,显然非对称加密算法的安全性更好。由于 RSA 加密算法技术成熟,是企业级加密标准,因此,文中采用 RSA 算法的数字签名方案对数据进行签名。签名与验证过程如下:

首先,要明确一些定义。

假设 n 是两个不同的奇素数 p 和 q 的乘积,即 $n = pq, \varphi(n) = (p - 1)(q - 1)$ 。

定义密钥空间:

$$k = \{ (n, p, q, d, e) \mid n = pq, p \text{ 和 } q \text{ 是素数}, de \equiv$$

$1 \bmod \varphi(n)$, e 为随机数}

对每一个 $k = (n, p, q, d, e)$, 定义加密变换为 $E_k(y) = y^b \bmod n, y \in Z_n$, 解密变换为 $D_k(x) = x^e \bmod n, x \in Z_n$, 其中 Z_n 为整数集合。公开 n 和 b , 保密 p, q 和 e 。

在上述定义的基础上, RSA 数字签名算法的过程为:

对明文 m 用解密变换作运算: $S \equiv D_k(m) = m^e \bmod n$ 。其中 d, n 为发送者 A 的私钥。接收者 B 收到签名后利用 A 的公钥和加密变换算法得到明文: $E_k(S) = E_k(D_k(m)) = (m^d)^e \bmod n$, 又 $de \equiv 1 \bmod \varphi(n)$, 即 $de = 1\varphi(n) + 1$, 根据欧拉定理 $m^{\varphi(n)} = 1 \bmod n$, 所以有 $E_k(S) = m^{e\varphi(n)+e} = [m^{\varphi(n)}]^e m = m \bmod n$ 。接收者利用接收到的明文 m 和签名 S 来验证此消息是否由 A 发送。

由于除了 A 之外, 没有用户拥有 e , 所以其他人不能产生 S , 因此 RSA 数字签名方案是可行的。

3.2 安全接入机制的实现

在认证过程开始之前, 必须有注册过程和密钥分配过程。注册步骤如图 4 所示, 注册完成之后, 采用密钥预分配机制完成每个节点的密钥对分配。

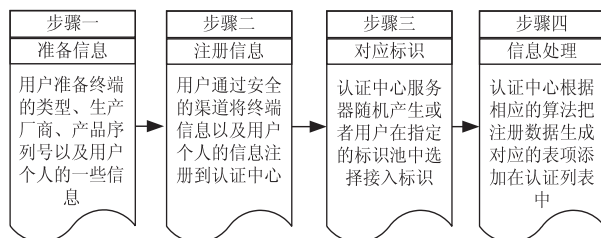


图4 注册过程

认证过程的通信流程如图 5 所示。

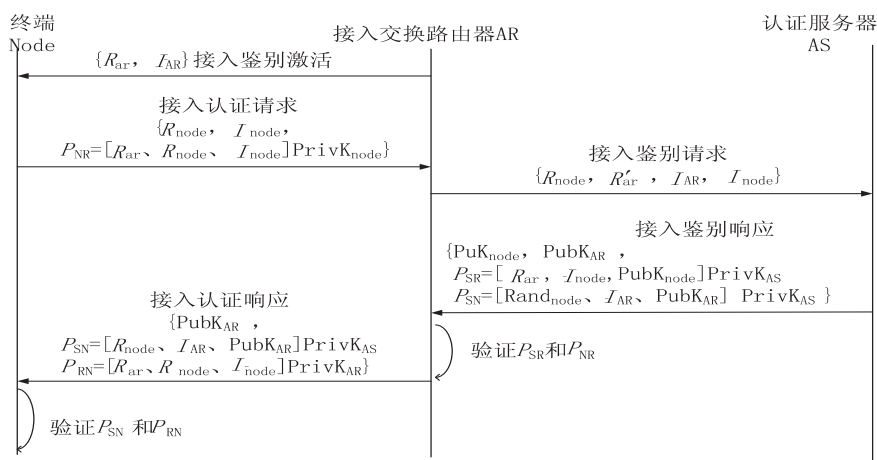


图5 安全接入机制

该控制机制作用于网络层, 所定义的安全协议报文传递时, 使用数据报文。为了能够接入网络, 完成终端和接入交换路由器之间的相互鉴定, 三个认证实体之间需要完成以下认证过程:

(1) AR 收到来自 Node 的接入鉴别请求分组后, 向 Node 发送接入鉴别激活分组以激活整个鉴别过程, 发送的鉴别分组中包括 AR 产生的随机数 R_{ar} 和 AR 的身份标识 I_{ar} 。

(2) 终端构造接入鉴别请求分组发送给接入交换路由器, 其中包括 Node 产生的随机数 R_{node} , Node 的身份标识 I_{node} 以及 P_{Nac} 。其中, P_{Nac} 是 Node 使用自己的私钥对 R_{node} 、 I_{node} 以及 R_{ar} 的签名。

(3) AR 接收到接入鉴别请求分组后, 向 AS 返回身份鉴别请求分组, 此分组中数据由 Node 的身份标识 I_{node} 、随机数 R_{node} , AR 的身份标识 I_{ar} 、随机数 R'_{ar} 组成。

(4) 终端与接入交换路由器的身份鉴别都由 AS 来完成, 当 AS 收到来自 AR 的身份鉴别请求数据包

后, 以 I_{node} 、 I_{ar} 为索引在数据库中得到 Node 和 AR 的有效公钥 PuK_{node} 、 PuK_{ar} , 验证 Node 和 AR 的身份。验证成功后向 AR 返回鉴别成功响应数据包, 数据中包括有效公钥 PuK_{node} 、 PuK_{ar} 、 P_{AA} 和 P_{AN} , 其中 P_{AA} 为使用 AS 的私有密钥对 R'_{ar} 、 I_{node} 、 PuK_{node} 进行签名, P_{AN} 为使用 AS 的私有密钥对 R_{node} 、 I_{ar} 、 PuK_{ar} 进行签名。

(5) AR 收到来自 AS 的身份鉴别响应数据分组后, 利用 AS 的公共密钥判断 P_{AA} 中的随机数 R'_{ar} 和步骤 (3) 中发送的随机数 R'_{ar} 是否一致, 以此来验证 P_{AA} , 然后利用 P_{AA} 中 PuK_{node} 验证 P_{Nar} : 匹配 AR 的身份标识和步骤 (1) 中发送的 I_{ar} , 校验在步骤 (1) 中发送的 R_{ar} 与步骤 (2) 中发送的 R_{ar} 相一致。若两者都一致, 则成功获得 PuK_{node} 。

(6) AR 发送接入响应分组到终端 Node, 接入响应分组数据中包括 AR 公钥 PuK_{ar} 、 P_{ArN} 和 P_{AN} 。 P_{ArN} 为 AR 的私有密钥对 R_{ar} 、 R_{node} 、 I_{node} 的签名。

(7) 终端 Node 对来自 AR 的接入响应做如下处理: 先校验步骤 (2) 中发送的 R_{node} 与 AS 私钥签名 P_{AN}

中的 R_{node} 是否一致,通过此结果验证签名;然后通过 PuK_{ar} 验证 PuK_{AN} ,验证方法是检查签名中的 I_{node} 与 Node 的身份标识 I_{node} 相一致,校验步骤(2)中发送的随机数 R_{node} 与包含在 AR 签名中的随机数相一致,若以上验证都顺利,则成功获得 PuK_{ar} 。

完成以上校验步骤后,AR 和 Node 通过 AS 实现了双向身份鉴别,获得了对方的公钥。Node 可以安全接入 AR,在验证 AR 的安全性之后,也防止 Node 登录到不安全的 AR。

4 性能及安全分析

4.1 性能分析

在该安全接入机制中,每个终端都要存储两部分信息:身份标识及其公私钥对、AS 及 AR 的公钥。对于终端来讲这样的内存开销是可以接受的。

RSA 算法在能耗方面很有优势。在整个认证过程中,Node 和 AR 所需的加密时间很短,基本可以忽略不计。这体现了 RSA 加密算法的优越性。

4.2 安全性分析

基于三元对等鉴别的一体化标识网络安全接入机制,满足了接入网中终端安全接入的需求,也满足了以下常见的安全性要求:

(1)防 DOS 攻击。

DOS 攻击即拒绝服务攻击,是一种非常普遍的网络攻击手段。攻击者利用网络设备的缺陷,持续向接入设备发送大量无用消息,接入设备由于忙于处理这些非法消息而不能处理其他合法的请求消息。该机制在认证过程中,加入实体产生的随机数,通过随机数验证之后才会对此消息进行处理。这一措施可以有效预防 DOS 攻击。

(2)防重放攻击。

重放攻击是指恶意终端通过重复发送合法终端或接入交换路由器发送过的消息来骗取对方的信任。在本方案中,可以通过设置随机数的生存时间来达到防重放攻击的目的,即只有在有效的生存时间内发送的消息才能被接收方认可。

(3)防中间人攻击。

中间人攻击即攻击者通过篡改接收到的对认证过程十分重要的合法信息,转发给接收方,并导致认证失败的攻击方式。在本机制中,由于使用 RSA 签名算法,接收方对收到的信息都会进行签名验证,通过验证签名算法中的随机数,能有效地防止中间人攻击。

5 结束语

由于一体化标识网络对网络安全的高要求,同时接入网的开放性和终端多样性使得其面临巨大的安全挑战,因此提升终端接入机制的安全性很有必要。文中借鉴三元对等鉴别机制,提出了一体化网络中的安全接入机制,采用了目前接受度最高的 RSA 签名算法,保证了其可行性。从 DOS 攻击、重放攻击、中间人攻击方面分析了该接入机制的安全性。研究一体化标识网络的通信安全机制将是下一步工作方向。

参考文献:

- [1] 王 上. 一体化网络接入交换路由器分离映射的设计与实现[D]. 北京:北京交通大学,2008.
- [2] 郑丽娟. 身份与位置分离网络中认证协议的研究与设计[D]. 北京:北京交通大学,2013.
- [3] Callegati F, Cerroni W, Ramilli M. Man-in-the-middle attack to the HTTPS protocol[J]. IEEE Security & Privacy, 2009, 7(1):78-81.
- [4] Sung M, Xu J. IP traceback-based intelligent packet filtering: a novel technique for defending against internet DDos attacks[J]. IEEE Transactions on Parallel and Distributed Systems, 2003, 14(9):861-872.
- [5] 罗洪斌,王洪超,张宏科,等. 基于标识的一体化网络终端统一接入控制方法:中国,2007101217453[P]. 2008-02-06.
- [6] 万 明,周华春,刘 颖,等. 基于身份标签的一体化网络接入认证方案[J]. 铁道学报,2012,34(8):70-81.
- [7] 唐建强,刘 颖,周华春,等. 一种身份与位置分离环境下基于网络的安全移动性管理协议[J]. 电子与信息学报,2013,35(1):151-158.
- [8] Postel J. IP internet protocol version 4[S]. [s.l.]:IETF, 1981.
- [9] Deering S E, Hinden R M. Internet Protocol, Version 6 (IPv6) specification[S]. [s.l.]:IETF, 1998.
- [10] 西安西电捷通无线网络通信有限公司. 一种基于三元对等鉴别(TePA)的可信平台验证方法:中国,200810232093[P]. 2010-01-13.
- [11] 黄振海,赖晓龙,铁满霞,等. 三元对等鉴别及访问控制方法国际提案进展[J]. 信息技术与标准化,2009(6):21-23.
- [12] 杨年鹏,龙昭华,蒋贵全,等. 基于虎符 TePA 的物联网安全接入机制研究[J]. 计算机工程与设计,2012,33(4):1305-1309.
- [13] 唐 鼎,赵海滨,侯自强,等. 独立于二层链路的接入认证[J]. 计算机工程,2006,32(4):184-186.