

# 可信的下一代互联网及其发展

## The Trustworthy Next-Generation Internet and Its Development

中图分类号: TP393 文献标识码: A 文章编号: 1009-6868 (2008) 01-0008-05

**摘要:** 目前下一代互联网技术中解决互联网的安全可信问题的研究还不充分。中国在可信下一代互联网方面已有一些研究进展。清华大学等单位完成的国家高技术研究发展计划资助项目(“863”计划)“可信下一代互联网关键技术及应用示范研究”针对当前互联网存在的安全可信问题,在重点解决互联网真实地址访问技术难题的基础上,设计和实现了可信的互联网基础设施、安全服务和典型应用的原型系统。可信下一代互联网有望为构造可信计算机网应用、可信电信网应用、可信广电网应用提供支持。

**关键词:** 可信互联网;下一代互联网;源地址验证

**Abstract:** Currently, the research on the security and credibility issues of the Next Generation Internet (NGI) is still insufficient. China has made some progress in the trustworthy NGI area. Institutes including Tsinghua University completed the National 863 High-tech Project, “Research on key technologies of trustworthy next generation Internet and application demonstration”, which focuses on the security and credibility issues of the current Internet. On this basis of source address validation technology, the project designed and implemented prototype systems of trustworthy Internet infrastructures, security services, and typical applications. The trustworthy NGI is expected to provide support for building of trustworthy computer network applications, trustworthy telecom network applications, and trustworthy IPTV network applications.

**Key words:** trustworthy Internet; next generation Internet; source address validation

吴建平/WU Jian-ping

毕军/BI Jun

(清华大学, 北京 100084)

(Tsinghua University, Beijing 100084, China)

于可信网络基础设施层面,也是可信网络其他层次的基础。从可信的角度出发,真实IP地址访问的问题实际上是地址的从属关系问题,也就是说:实体发出的报文应该只携带它拥有的地址,报文只应该被拥有其源地址的实体发出。在原来的互联网设计中,假设网络的所有设备(包括主机和路由器)都是可信的。而在目前复杂的网络环境下,对主机的信任已经不存在,所以必须依靠网络的基础设施来保证源地址的从属关系被实现。基于网络本身的分层结构,真实地址的访问体系结构被分为域间真实地址访问、域内真实地址访问和子网内真实地址访问3部分,他们有机地组合在一起,共同形成一个真实地址访问的框架。

通过实现真实地址的访问,能够带来如下的好处:

- 可以直接解决一些伪造源地址的分布式拒绝服务攻击(DDoS),比如Reflection攻击等。

- 真实地址访问,使得互联网中的流量更加容易追踪,使得设计安全机制和网络管理更加容易。

- 可以实现基于源地址的计费、管理和测量。

- 可以为安全服务和安全应用的设计提供支持

统一的用户标识和安全服务在可信下一代互联网的体系结构中,

互联网已经对人类生产生活乃至社会的进步产生了深刻的影响。但是,由于互联网体系结构所存在的固有缺陷,互联网在安全可信方面正面临前所未有的严峻挑战,已成为互联网应用发展的主要“瓶颈”问题之一。

未来5至10年内,互联网技术将进入更新换代的历史时期,以IPv6为基础的下一代互联网已经成为国际、国内的研究热点。可信的下一代互联网将重点解决下一代互联网的更安全更可信问题,应当具有如下主要特征:

(1) 确保网络地址及其位置的真

实可信

- 真实性: 网络基于真实IPv6地址访问。

- 追查性: 根据真实IPv6源地址可追查网络地址的真实位置。

- 监控性: 根据网络用户实体的真实位置可监测和控制网络用户实体的行为。

(2) 增强网络应用实体的真实可信

- 身份可信性: 真实IPv6源地址可增强网络用户实体身份的可信度。

- 应用安全性: 可支持安全可信的网络应用。

真实IPv6源地址寻址结构在可信的下一代互联网的体系结构中,属

属于真实地址访问之上的安全服务层。该安全服务层作为基础设施为应用层提供的一种公共的安全服务层,利用并封装底层基础设施提供的可信任功能,为可信任下一代互联网的典型应用提供统一的标识和认证服务。基于真实地址的实体身份标识、身份认证、可信域名服务、密钥管理服务是实现可信安全服务的基本安全服务。

从体系结构功能分层的角度出发,可以把安全服务层作为基础设施为应用层提供的一种公共的安全服务层,利用并封装底层基础设施提供的可信任功能,为可信任下一代互联网的典型应用提供统一的标识和认证服务。

可信任下一代互联网能够解决传统应用中的安全问题,实现可信的应用,例如可信任电子邮件、可信BBS和可信的SIP通信系统等。这些可信应用可以解决传统电子邮件系统中邮件地址的真实性问题;解决垃圾邮件的追查机制,杜绝垃圾邮件和邮件病毒;解决传统BBS系统中用户行为责任追溯和用户隐私保护之间的矛盾问题;解决SIP通信系统在可信网络的环境中的安全问题等。

## 1 国际相关研究

在网络安全服务体系结构领域,早在1988年,国际标准化组织ISO/IEC JTC1就对开放式系统参考模型增加了关于安全体系结构的描述,提出了5种安全服务(认证服务、保密性服务、完整性服务、访问控制服务、抗抵赖服务)和实现这些安全服务的安全机制,以及这些安全服务和安全机制在开放系统互连(OSI)不同协议层的功能分配。目前在互联网的研究组织IRTF和技术标准组织IETF中也对这个问题展开了工作。虽然RFC1287<sup>[1]</sup>中就已经指出了互联网安全参考模型的重要性,但至今仍然没有一个完整的安全体系结构模型。RFC2401只是IP层的安全框架,其他相关的RFC

主要针对各个具体问题提出具体的解决方法,这些安全技术相对独立,无法从整个体系上满足系统的安全性需求。目前一些技术研究仍然在进行当中,例如在研究网络中用户、主机的认证方面,主机身份协议(HIP)是其中的一个代表;在网络路由协议安全性方面,安全域间路由(SIDR)是其中的一个代表。

美国政府于1996年10月宣布启动下一代互联网(NGI)研究计划。作为NGI计划的一个补充部分,美国100多所大学于1996年底联合发起Internet2研究计划<sup>[2]</sup>,其目的是利用现有的网络技术来探索高速信息网络环境下的新一代网络应用,同时力图发现现有网络体系结构理论的缺陷部分,为新的信息网络理论研究提供需求依据。在Internet2所提出的下一代网络的体系结构中,中间件是在网络和应用之间为各种应用系统提供的一组公共的服务。Internet2中间件计划(I2-MI)正开始在Internet2上研究和部署网络中间件,向上层提供识别、验证、授权、目录和安全等方面的服务,其中主要是安全服务。

美国国防部国防先进研究计划局(DARPA)项目资助了由美国南加州大学信息科学研究所、麻省理工学院计算机科学实验室和伯克利加州大学国际计算机科学研究所共同参加的新一代Internet体系结构研究项目——NewArch<sup>[3]</sup>,开展新一代Internet的体系结构研究。该项目组最近的研究成果对目前的Internet进行了反思,提出了下一代互联网设计中的几条原则,例如面向变化的设计、可控制的透明性等。

在防止源地址假冒方面,目前国外的主要研究包括:

(1)IP层的安全通信协议(IPSec),它由认证头(AH)、封装安全净荷(ESP)和密钥管理框架(ISAKMP/IKE)组成,IPSec实现数据源发认证、保密和数据完整性。IETF规定在IPv6的实现中,IPSec是必须支持的。但是IPSec在性

能方面也存在严重的问题,即使丢弃了假冒分组,对系统带来的开销仍然很大,使DDoS等攻击仍然可以达到目的。另外核心网络中的路由器之间的流量很大,如果使用这种技术作为验证手段,对路由器的负担过大。

(2)假冒IP地址过滤技术代表性方案有入口过滤<sup>[4]</sup>、单播反向路径转发(uRPF)<sup>[5]</sup>、分布式分组过滤(DPF)<sup>[6]</sup>、源地址验证增强机制(SAVE<sup>[7]</sup>、iSAVE<sup>[8]</sup>)等。入口过滤要求设备制造商的支持和各个ISP间的合作以及全局部署;uRPF无法解决非对称路由的问题;DPF需要扩展BGP协议,当网络中的路由动态变化时可能导致丢弃正常的分组;SAVE要求全局部署;iSAVE的实现相对复杂。

(3)源地址追踪技术代表性的方案有SPIE<sup>[9]</sup>、iTrace<sup>[10]</sup>和概率分组标记<sup>[11]</sup>等,主要缺陷是回溯算法比较复杂,事后追溯而无法实时发现伪造源IP地址。其中概率分组标记类的算法无法应对单一分组地址欺骗的情况。

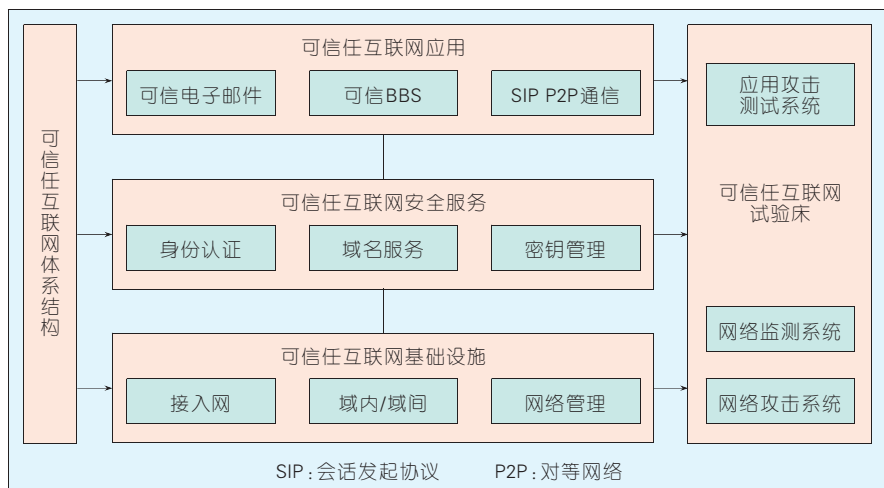
(4)网络接入控制技术,例如802.1x<sup>[12]</sup>等。但这些技术还不能完整地实现网络层的源地址假冒控制。

## 2 可信下一代互联网

在清华大学等单位承担的国家高技术研究发展计划资助项目(863计划)“可信下一代互联网关键技术及应用示范研究”中,针对目前互联网存在的安全性弱、可信度低、移动性和流媒体业务承载能力差等主要问题,在重点解决互联网真实地址访问技术难题的基础上,设计和实现了可信的互联网基础设施、安全服务和典型应用。目前其中一些关键技术已经制订了IETF RFC草案。

### 2.1 可信下一代互联网体系结构

可信的下一代互联网体系结构是一个层次模型,可以分为可信的网络基础设施层、可信的安全服务层和可信的互联网应用3个层次,利用基于真实IP地址的网络基础



▲图1 可信下一代互联网体系结构

设施,构建基于全局用户标识的可信任的安全服务,实现可信的下一代互联网应用,如图1所示。

## 2.2 基于真实IPv6地址的互联网基础设施

当前互联网面临着各种由于缺少信任而带来的问题。路由转发基于目的地址,对于源地址不做检查,使得伪造源地址攻击轻易而频繁。在互联网中地址是主机的标识,而缺乏源地址的验证,使得无法在网络层建立起信任关系。通过实现真实地址寻址结构,能够带来如下的收益:

- (1)可以解决一些伪造源地址的DDoS攻击,比如Reflection攻击等。
- (2)真实地址访问,使得互联网中的流量更加容易追踪,使得设计安全机制和网络管理更加容易。
- (3)可以实现基于源地址的计费、管理和测量。
- (4)可以为安全服务和安全应用的设计提供支持。

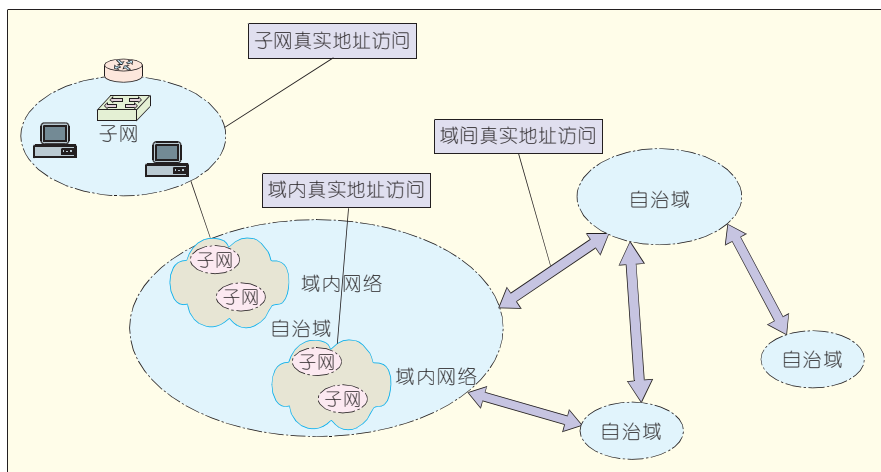
基于网络本身的分层结构,真实地址的访问体系结构被分为域间真实地址访问、域内真实地址访问和子网内真实地址访问的3部分,他们有机地组合在一起,共同形成一个真实地址访问的框架,如图2所示。

域间真实地址方法实现AS(自治系统)粒度的真实地址验证功能。根

据验证规则的生成方式,设计实现了两类方法:基于路径信息方法和基于端到端轻量级签名的方法。前一种方法适合于邻接部署,后一种方法适合于非邻接部署。

域内真实地址方法实现地址前缀级的真实地址验证功能。设计了基于路径和距离的反向地址查找机制和源地址验证模块,可以部署在边缘路由器或域内路由器上。

子网内真实地址方法保证在网络中的报文应该来自拥有该报文源地址所有权的某子网内的主机。针对不同的部署能力,设计了两类方法:IPv6真实地址分配和接入交换机的准入控制机制;主机与安全网关之间端到端的认证机制。



▲图2 真实IPv6地址寻址结构

与国际上各种源地址假冒防御机制相比,上述这些机制和协议具有简单高效、松耦合、多重防御、支持增量部署和激励机制等优点,形成了一个完整的系统解决方案。

## 2.3 可信下一代互联网安全服务

从体系结构功能分层的角度出发,把安全服务层作为基础设施为应用层提供的一种公共的安全服务层,利用并封装底层基础设施提供的可信任功能,为下一代互联网的典型应用提供统一的标识和认证服务。

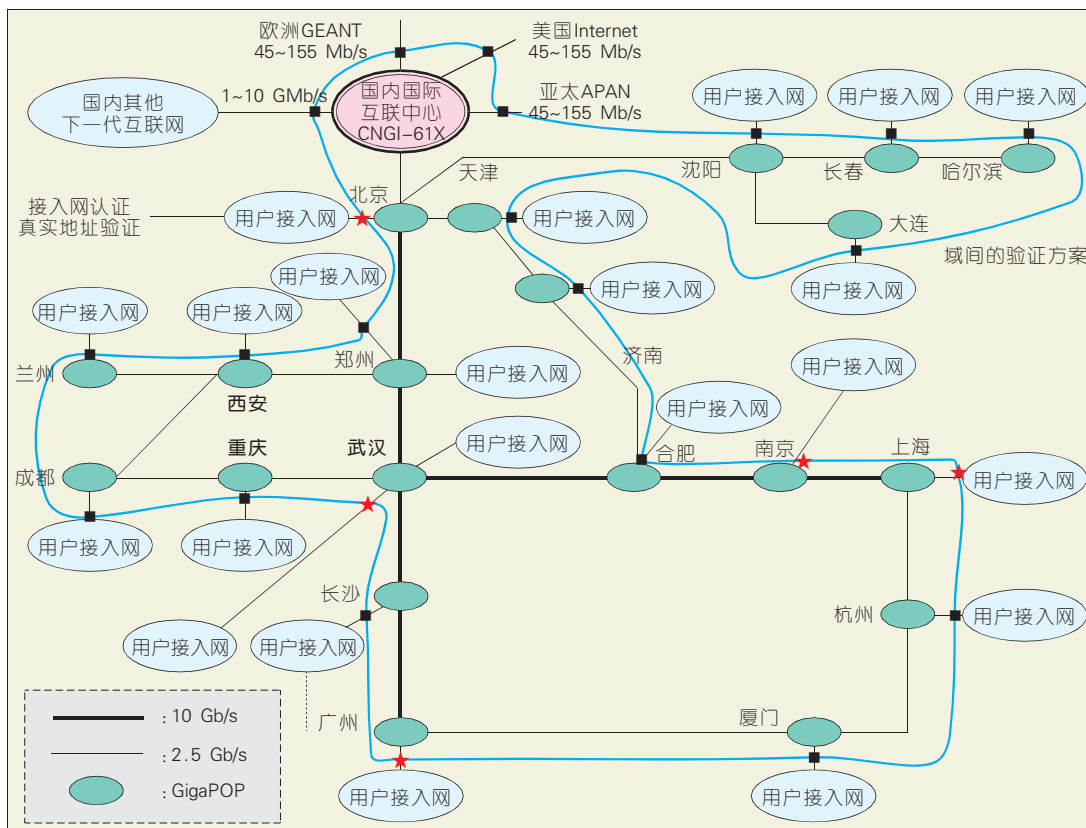
选择域名系统作为统一的用户标识,选择远程拨号用户认证(RADIUS)和Diameter协议作为管理域内的认证标准,选择DNS安全扩展(DNSSec)结合传统公钥基础设施(PKI)作为密钥管理的基础设施。

基于真实地址的实体身份标识、身份认证、可信域名服务、密钥管理服务是实现可信安全服务的基本安全服务。

在真实地址和标识的互联网环境下,应用系统的体系结构、认证和密钥管理的方式都可以得到简化,主要体现在以下几个方面:

- (1)利用域名系统实现统一的实体标识,实现跨管理域的分布式应用。由于域名系统是可扩展的、比较成熟的标识体系,借助域名系统实现的统一实体标识体系也具有良好





▲图3 基于CNGI- CERNET2的可信任下一代互联网试验床

可扩展性,而且用户容易接受、容易记忆。

(2) 利用安全服务提供统一标识和跨域的身份认证,而不需要每个应用系统分别实现各自的认证系统。

(3) 通过域名服务提供的密钥管理机制,可以实现灵活的、可扩展的密钥管理和协商方式。

## 2.4 可信下一代互联网典型应用

在可信下一代互联网典型应用中设计和实现了基于真实地址的可信任电子邮件、可信BBS和可信SIP通信系统等领域的研究与系统开发工作。以真实地址基础设施和安全服务为基础,解决了一些在传统应用系统中无法解决的关键问题:

- 解决了传统电子邮件系统中邮件地址的真实性问题;
- 解决了垃圾邮件的追查机制,杜绝了垃圾邮件和邮件病毒;
- 解决了传统BBS系统中用户行

为责任追溯和用户隐私保护之间的矛盾问题;

- 解决了SIP通信系统在可信网络的环境的安全问题,如假冒服务、拆卸会话等;
- 基于真实域名服务器(DNS)的服务,解决了SIP通信系统体系结构和信令过程的优化问题。

## 2.5 可信下一代互联网试验床

目前基于CNGI-CERNET2已经部署了包含12个真实地址实验自治系统的可信下一代互联网试验床。其中部署了真实地址网络设备原型系统,流量监控系统,可信安全服务系统,可信电子邮件、BBS和VOIP等应用,如图3所示。

## 3 可信下一代互联网的发展趋势

近一两年来,国际上陆续开展了一些新的研究计划。其中比较著名的

是美国自然科学基金会(NSF)启动的GENI<sup>[13]</sup>和FIND<sup>[14]</sup>研究计划。GENI试图发现和评估可以作为21世纪互联网基础的新的革命性概念、示范和技术,建立一个支持新网络体系结构探索和评估的大规模试验环境,他们期望未来的互联网具有以下特点:值得社会信任,激发科学和工程革命,支持新技术融合,支持普适计算,成为物理世界和虚拟世界的桥梁,支持革命性服务和应用。FIND是美国NSF另外一个研究计划。美国的科学家已经在考虑从现在开始15年内全球互联网是什么样子,以面向端到端

的体系结构为基础,研究传感器系统网络(NOSS)、可编程的无线通信、广义联网。美国试图通过这些前瞻性的研究计划保持其在信息技术和互联网领域的领导地位。虽然目前这些计划还没有取得实质性成果,但从其研究计划中可以看到可信互联网是其中的重要课题。例如其中一些研究者提出了Passport结构<sup>[15]</sup>。

可以预见,未来可信互联网的研究,主要涉及以下几个方面的技术研究:

- 可信下一代互联网体系结构和标准体系,以可信互联网为基础支持“三网合一”;
- 可信下一代互联网真实地址关键技术,以及支持真实地址的路由器、交换机和专用网络设备;
- 基于可信下一代互联网的全局标识的安全服务;
- 可信下一代互联网应用,包括P2P应用,IPTV和互动电视,无线和

移动应用;

- 从当前互联网向可信下一代互联网过渡的技术;

- 大规模的可信任下一代互联网试验网。

#### 4 结束语

以IPv6为基础的下一代互联网已经成为国际国内的研究热点之一,但是目前下一代互联网技术中解决互联网的安全可信问题的研究还不充分。针对这个问题,中国在过去几年里已经取得了一些初步研究成果,正在继续深入开展。中国发展可信下一代互联网是保证国家信息基础设施和网络应用的安全可信的需要,符合国家的创新发展战略,可以带动中国科技和产业化发展。

随着互联网特别是下一代互联网的发展,IPv6协议将成为三网融合的基础。以可信下一代互联网为基础,可有望为构造可信计算机网应用、可信电信网应用、可信广电网应用提供支持。

可信网络的研究还存在许多值得进一步深入研究的地方,希望有更多的研究者可以加入到可信网络的研究和建设中来。

#### 5 参考文献

[1] KENT S, ATKINSON R. Security architecture

for the Internet protocol [R]. RFC2401, 1998.

[2] Building Tomorrow's Internet [EB/OL]. <http://www.internet2.org/>.

[3] NewArch Project: Future-Generation Internet Architecture [EB/OL]. <http://www.isi.edu/newarch/>.

[4] FERGUSON P, SENIE D. Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing [R]. RFC2827, 2000.

[5] BAKER F, SAVOLA P. Ingress filtering for multihomed networks [R]. RFC3704, 2004.

[6] PARK K, LEE H. On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law Internets [C]// Proceedings of Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication (SIGCOMM 2001), Aug 27-31, 2001, San Diego, CA, USA. New York, NY, USA: ACM, 2001:15-26.

[7] LI J, MIRKOVIC J, WANG M P, et al. SAVE: source address validity enforcement protocol [C]// Proceedings of IEEE Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2002): Vol3, Jun 23-27, 2002, New York, NY, USA. Piscataway, NJ, USA: IEEE, 2002:1557-1566.

[8] MIRKOVIC J, XU ZHIGUO, LI JUN, et al. iSAVE: incrementally deployable source address validation [R]. CSD-TR-020030. Los Angeles, CA, USA: University of California, 2002.

[9] SNOEREN A C, PARTRIDGE C, LUIS A, et al. Hash-based IP traceback [C]// Proceedings of Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication (SIGCOMM 2001), Aug 27-31, 2001, San Diego, CA, USA. New York, NY, USA: ACM, 2001:3-14.

[10] BELLOVIN S, LEECH M, TAYLOR T. ICMP traceback messages [R]. RFC2026, 2003.

[11] SAVAGE S, WETHERALL D, KARLIN A, et al. Practical network support for IP traceback [C]// Proceedings of Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication (SIGCOMM 2000), Aug 28-Sep 1, 2000, Stockholm, Sweden. New York, NY, USA:

ACM, 2000: 295-306.

[12] CONGDON P, ABOBA B, SMITH A, et al. IEEE 802.1X Remote authentication dial in user, service (RADIUS) usage guidelines. RFC3580, 2003.

[13] GENI net Global Environment for Network Innovations [EB/OL]. <http://www.geni.net/>.

[14] NSF NeTS FIND Initiative [EB/OL]. <http://www.nets-find.net/>.

[15] LIU XIN, YANG XIAOWEI. Efficient and secure source authentication with packet passports [C]// Proceedings of the 2nd conference on Steps to Reducing Unwanted Traffic on the Internet (SRUTI 2006): Vol2, Jul 6-7, 2006, San Jose, CA, USA. 2006: 7-13.

收稿日期:2007-12-09

#### 作者简介



吴建平, 中国教育和科研计算机网专家委员会主任, 中国教育和科研计算机网网络工程研究中心主任、教授、博士生导师。目前主要研究领域为互联网、高性能网络、网络协议工程学等。



毕军, 清华大学信息网络工程研究中心网络体系结构和IPv6研究室主任、教授、博士生导师。美国贝尔实验室博士后。主要研究领域为互联网体系结构和协议、下一代互联网和IPv6、高性能网络互联系统等。

#### 中兴通讯首获CIMA最佳中国合作雇主奖

2007年11月26日获悉,在全球拥有16万成员的著名管理会计师公会——英国皇家特许会计师公会(CIMA)首次在中国上海举行“最佳中国合作雇主颁奖仪式”。中兴通讯等三家企业获得“2007CIMA最佳中国合作雇主企业”这一全球性管理会计大奖,这是中国本土企业首次获得此殊荣。

中兴通讯高级副总裁、财务总监韦在胜出席了颁奖仪式,并作为第一家获奖企业上台发言。该奖项是CIMA皇家特许管理会计师公会全球总部授予那些在中国境内重视人才培养、财务管理先进,且具有前瞻性发展战略

略的合作雇主企业的最高荣誉。与往年不同的是,2007年CIMA全球总部将年度大奖颁发给了中国的领先企业。

CIMA指出,中兴通讯能卓有成效地利用国内市场赋予的低成本优势和海外市场的发展机遇,通过管理和技术创新,大力开拓国际市场,在不断巩固和扩大国内市场份额的同时,成为为数不多的真正“走出去”实现国际化运营的国内企业之一。同时,中兴通讯在财务管理人才方面,实行先进的国际化战略,实现了财务稳定和价值创造。业内人士称,此项荣誉树立了中兴通讯尊重人才的企业形象,也代表中兴通讯财务人员正以卓越的成就和素质赢得更多的国际认同。