DOI:10.3969/j.issn.1009-6868.2017.03.013
网络出版地址:http://www.cnki.net/kcms/detail/34.1228.tn.20160426.1453.002.html

# 一种可信身份网络架构及在互联网安全中的应用

# A Network Architecture Based on Trusted Identity and Its Applications

中图分类号:TN929.5 文献标志码:A 文章编号:1009-6868 (2017) 03-0058-004

**摘要:** 提出了一种基于身份和位置分离思想的网络架构,确保用户身份标识的真实可信,并在结构上将用户和核心网络隔离,屏蔽用户侧攻击,提升了网络的安全性能。认为基于身份标识的网络安全管理应用可以提高网络的攻击源识别能力和溯源效率,实现主动防御;同时,这种虚拟身份和可信身份的绑定,既能丰富互联网应用,又有助于实现网络信息的分级保护,净化网络环境。

**关键词:** 可信身份网络;身份标识;位置标识;网络安全

**Abstract:** A network architecture based on separation of location and identity is proposed in this paper. Under the architecture, user identity is trusted, isolation between user side and core network side is achieved. Thus, network attack from user side is avoided, the security performance is promoted. Additionally, security management applications based on the architecture can both improve the capability of attack source identification and boost the efficiency of source tracing. Meanwhile, it can not only enrich internet applications, but also realize the hierarchical protection of network information to clean network environment.

**Key words:** trusted identity network; access identifier; router identifier; network security

*毛玉欣/MAO Yuxin* [1]
*郝振武/HAO Zhenwu* [1,3]
*江家仁/JIANG Jiaren* [2]

(1. 中兴通讯股份有限公司,江苏 南京 210012;
2. 中国电信股份有限公司上海研究院,上海 200122;
3. 移动网络和移动多媒体技术国家重点实验室,广东 深圳 518057)
(1. ZTE Corporation, Nanjing 210012, China;
2. Shanghai Research Institute of China Telecom Co. Ltd, Shanghai 200122, China;
3. State Key Laboratory of Mobile Network and Mobile Multimedia Technology, Shenzhen 518057, China)

近年来,网络技术的不断升级以及智能终端的迅猛发展带动了移动互联网的迅速普及,越来越多的人通过各种移动终端接入到互联网,获取网络资源。中国互联网络信息中心(CNNIC)的一项调查显示[1],截止2014年,中国网民总体规模达到6.49亿,其中使用移动终端的网民就达到5.57亿,占比85.8%。移动互联网已成为社会活动不可缺少的部分。

## 1 互联网安全现状和分析

快速发展的移动互联网给人们的生产和生活带来了便利,也产生了很多安全威胁。2014年有46.3%的用户遭遇过网络安全问题,其中病毒木马入侵、账号密码被盗情况最为严重,分别达到26.7%和25.9%,网络欺诈比例为12.6%[1]。一方面,人们的生活正变得越来越离不开网络;另一方面,使用人群中认为网络非常不安全或者不太安全的也已接近半数。在网络发展和使用不可逆转的形势下,改善网络安全,增强网络可信性是一项具有重大意义且亟待解决的课题。

通过对众多网络安全事件的剖析,发现虚拟性和匿名性[2]是引发网络安全威胁的重要因素。如今的互联网已经构建了一个庞大的虚拟空间,现实社会中的很多活动都可在其中进行,例如,网络购物、网上支付、网络理财、网络聊天等。这一系列活动都以匿名方式进行,通信双方和通信设备都无法获知对方的真实身份。匿名给网络攻击提供了广泛空间,攻击者可通过模拟他人虚拟身份进行信息窃取、诈骗,虚假言论传播等活动,给社会经济造成巨大损失,而网络监管机构对此尚缺乏及时有效的管理和控制手段。

网络信息安全管理存在缺陷主要表现在:

(1)用户在网络活动中以多个身份存在[3]。在网络层通常以IP标识身份,在应用层通常以不同的用户名标识身份,各身份标识之间缺乏有效的统一和关联。这种用户身份标识的不唯一、不统一给管理带来了巨大困难。依据网络身份溯源用户真实身份的链条极长,机制极其复杂。一旦有安全事件发生,管理者很难及

收稿时间:2016-03-02
网络出版时间:2016-04-26

时、准确地追溯到攻击源。

（2）用户身份标识可随时改变或被篡改、伪装，对身份标识缺乏有效约束。IP地址作为用户在网络层的身份标识可随时间、地点、接入方式的变化而改变；用户的账号信息也能轻易被攻击者注册或仿冒，这就势必造成管理主体模糊，加大了网络监管难度。对身份标识缺乏约束，降低了标识信息的真实性，从而可能导致对某些安全事件根本无法实施溯源[4]。

（3）网络安全防御措施跟不上安全事件的发展[5]，对于网络安全事件的防御始终处于被动状态。一旦有新的攻击方式出现，通常需要投入大量的人力、物力分析查找原因，升级软硬件，防御成本过高。这种攻防成本不对称的状况助长了各种安全事件频出，严重影响到网络的可信性。

应对上述安全缺陷的一种方式是推行网络实名制管理[6]。实践表明现有的一些实名制管理方式仍然面临一些难题。例如：通过用户上传身份登记信息的方式实现身份实名，这种方式获取的身份信息真伪难辨，无法判断用户自身上传的信息是否真实可信[7]。又或是在网络内容提供商（ICP）侧推行应用层实名制，这种实现方式通过ICP保存用户真实身份信息，但ICP本身也难以保证安全可靠，容易发生信息泄漏[8]。另外由于业务种类和ICP数量众多，且新业务和新ICP层出不穷，这给实名制的管理维护也带来了很大困难。

## 2 基于标识的可信身份网络设计

### 2.1 IP地址语义过载

互联网使用传输控制/网络通信协议（TCP/IP），IP在其中承载了双重语义[9-10]：一方面IP地址充当了主机身份标识，用于在通信过程表示会话的端点；另一方面IP地址又作为位置标识，在路由系统中被用于数据包的寻址转发。这种双重语义在互联网使用之初并没有产生安全问题，因为最初的互联网是面向科学研究，而非商业应用设计的，设计者认为使用互联网的终端是静止的、安全的、可信任的[11]。但随着互联网被推向商业社会，移动人群成为网络的主流使用者，互联网使用场景发生了变化，而TCP/IP却没有发生本质改变。移动互联网时代，IP地址作为位置标识，在用户位置改变时也要随之改变，否则无法进行数据包的正确路由；作为用户身份属性，又要求无论用户位置怎么改变其IP地址保持不变[12]。IP双重语义引发的矛盾随之凸显，用IP标识用户身份属性也变得不再可信。

### 2.2 可信身份网络设计

针对IP集成身份和位置双重属性的缺陷，设计了一种基于身份和位置分离思想[13-14]的可信身份网络。可信身份网络将用户的身份标识和位置标识分别用接入标识（AID）和路由标识（RID）表示，网络从功能上抽象为接入服务节点（ASN）和身份位置寄存器（ILR）两部分。AID和RID的作用如下：

（1）AID在用户开户过程中由网络管理者根据用户真实身份分配、管理，作为用户接入网络的身份标识。AID与用户身份信息绑定，作为开户信息保持不变。用户接入网络时，通过基础网络的认证机制实现用户合法性认证后，才能被赋予对应的AID，以保证AID作为身份标识可信。

（2）RID用于标识用户当前接入位置。在用户初始接入网络或者移动过程中，由为用户接入服务的ASN为用户分配和管理RID。当用户从一个ASN移动到新的ASN接入时，需要由新的ASN重新为用户分配新的接入位置标识RID。

可信身份网络架构中，ILR用于记录用户的（AID，RID）映射关系。多个ILR构成映射网络，集中管理网络中所有用户的映射关系。用户初始接入网络时，ASN需要生成映射关系（AID，RID），并将映射关系上报给ILR。用户移动过程中一旦发生RID更新，需要及时通知ILR更新映射关系，以保证映射网络中每个用户的（AID，RID）映射关系都能表示用户当前的接入位置。

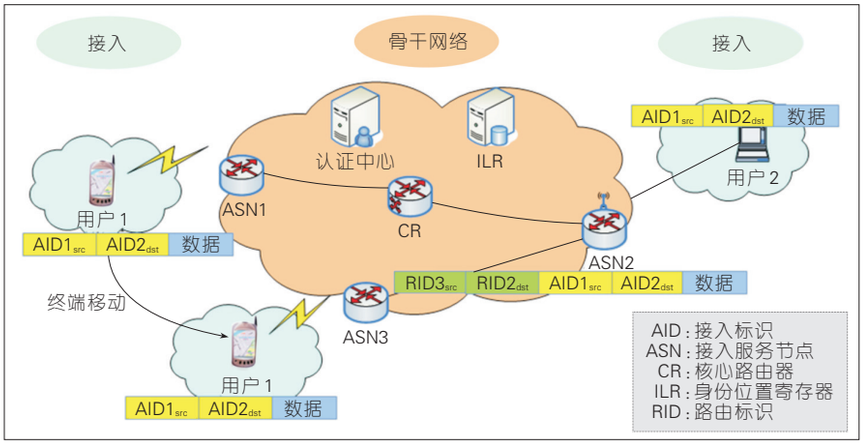
可信身份网络架构下的通信过程如图1所示：

用户在发生跨ASN的移动时，ILR需要及时更新用户的映射关系。例如用户1初始通过ASN1接入网络，ASN1需要将用户1的映射关系（AID1，RID1）上报给ILR。当用户1从ASN1接入移动到ASN3接入，ASN3需要将用户1的最新映射关系（AID1，RID3）上报给ILR，ILR用最新的映射关系替代原有的映射关系，并通知ASN1解除用户1的映射关系。用户1向用户2发起通信，只需知道用户2的身份标识AID2，而不需要知道用户2的当前接入位置，即用户1无论在什么位置，发送的报文始终以源地址AID1，目的地址AID2封装。假设用户1从ASN1移动到ASN3接入，并向用户2发起通信，ASN3接收用户1的报文后，通过向ILR查询获知用户2的映射关系（AID2，RID2）。ASN3在上述报文外层用源地址RID3目的地址RID2进行封装。此后，路由系统根据目的地址RID2将所述报文路由转发至用户2当前接入所使用的ASN2，ASN2将报文作解封装处理后发送给用户2。

上述通信过程中的数据包在核心网络中根据RID进行路由，AID仅标识用户身份，不参与路由过程。用户只有通过合法性认证才被赋予对应AID，保证身份标识的可信。可信身份网络中的身份标识由运营商集中管理维护，可应用于所有互联网业务。在通信实现过程中，AID、RID可以继承基于IP的路由编号机制，使身份信息不易被用户感知。

### 2.3 可信身份网络的安全优势

可信身份网络将身份属性和位




▲图 1 可信身份网络通信过程示意

置属性作了彻底分离，在基础网络层面建立了统一的身份标识体系，一定程度上解决了传统网络长久面临的安全隐患。如图 2 所示，可信身份网络安全模式主要体现在：

（1）身份标识唯一真实可信。网络为用户在全网范围内分配唯一的身份标识，且在开户过程中就将其与用户身份信息进行强关联。用户经过合法性认证后，才可使用身份标识开展业务。身份标识的唯一性、真实性、防冒用、防篡改保证了用户从事网络活动时身份的可信性。

（2）AID 和 RID 的作用域使得用户和核心网络形成逻辑隔离。身份标识作用于用户和 ASN 之间的接入网络，位置标识作用于各 ASN 组成的核心网络。AID 和 RID 作用域的区分实现了网络拓扑对用户的隐藏。用户只能使用身份标识发起通信，无法获知位置标识，这就使得用户无法直接访问中间网络设备，避免了网络设备遭受用户侧直接攻击。

（3）通信过程中每个数据包都携带身份标识 AID，便于网络管理。可信身份网络中的每个数据包都封装有 AID 标识，且实现端到端传递。无论用户的接入时间、地点等接入条件是否改变，数据包携带的 AID 都不会发生变化，因此一旦网络设备发现恶意用户的攻击，就可根据 AID 对其实施有效阻止，而不会影响到网内的其他用户，便于网络实施主动防御。

可信身份网络使用身份标识 AID 实现网络实名制，如表 1 所示，与现有网络实名制体系[15]比较，这种实现机制存在众多优势。

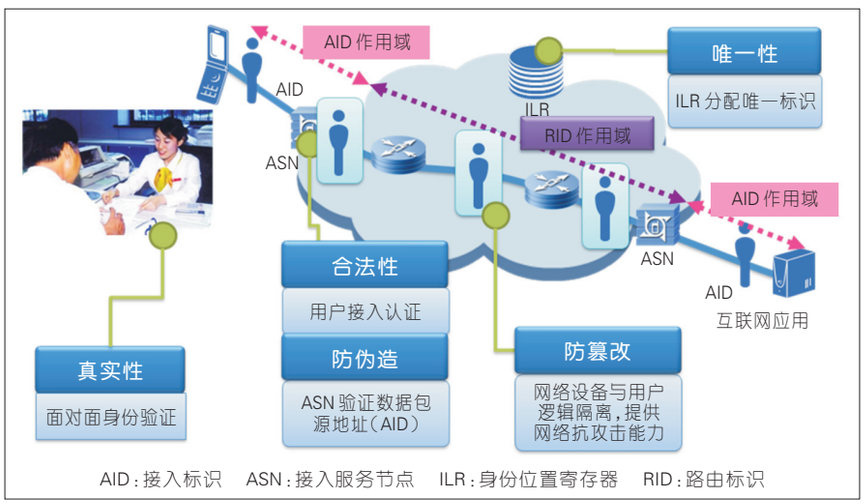
## 3 基于可信身份网络的安全应用

图 3 给出了基于可信身份标识的安全管理应用。在可信身份网络架构下，用户和 ICP 在申请接入网络时，都需要进行实名验证。网络运营商根据用户和 ICP 提交的身份信息，向监管中心提请身份验证。监管中心可根据用户或 ICP 的诚信档案、身份信息等对其进行合法性验证。验证通过之后，通知网络为用户或 ICP 分配身份标识 AID，网络将分配给用户或 ICP 的 AID 同时报送给监管中心，在监管中心实现用户或 ICP 的身份信息和 AID 的关联。由于可信身份网络架构中的每个通信数据包都携带 AID，因此可以基于 AID 对用户和 ICP 的网络行为进行管控。一旦发现有非法或可疑行为，网络可根据 AID 进行及时阻断，并可进一步根据 AID 进行跟踪溯源。

基于可信身份标识 AID 可开展一系列安全管理和应用，以改善网络安全性能：

（1）数据报文接收方可根据身份标识判断信息来源的可信性。网络管理者也可根据数据流中的身份标识对网络行为、网络内容进行快速溯源，对于非法行为进行及时阻断，快速识别攻击源，改进追溯机制，提高网络安全管理效率，压缩网络攻击的实施空间，扭转攻防成本不对称的局面。另外一旦发现恶意攻击，可直接屏蔽 AID 标识对应的攻击源，而无需对整个区域网络实施阻断，减少攻击处理所带来的负面影响。

（2）实现内容分级保护。可信身份标识在网络中是全程全网传递，运营商和 ICP 可根据身份标识识别用户的身份、年龄等特征，实现基于身份标识的内容分级提供，为不同的社会群体提供不同的网络信息，有利于

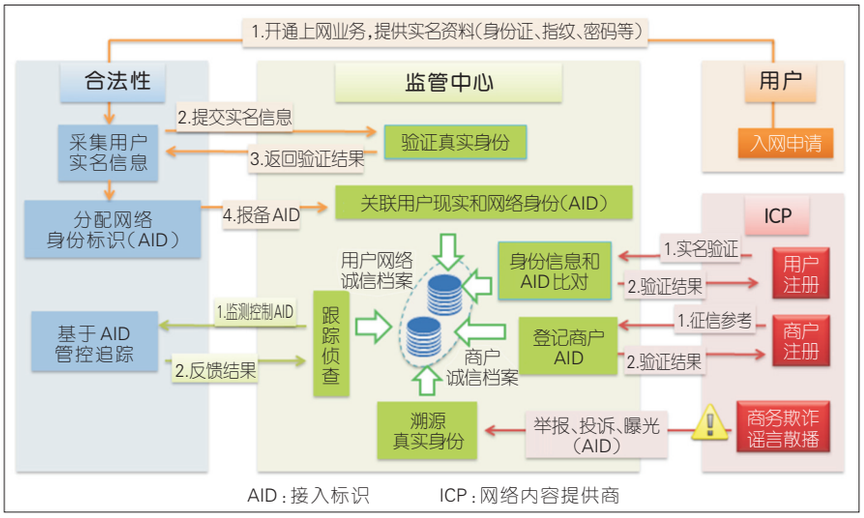



▲图 2 可信身份网络安全模式

▼表1 可信身份网络与现有网络实名制体系的比较

| | 现有网络实名制体系 | 可信身份网络实名机制 |
|---|---|---|
| 安全性 | 个人身份信息存放于ICP处，ICP众多，难以监管，容易造成信息泄漏 | 个人信息集中存放于运营商处，不对第三方开放，最大程度保护用户隐私 |
| 身份可信度 | 身份信息依赖用户注册上传，不可信，易篡改，真伪难辨 | 用户开户过程，需面对面进行身份验证确认，身份可信 |
| 实施对象数量 | ICP数量众多，且新业务、新ICP不断出现，身份信息难以管理维护 | 运营商在网络层一次性实施，应用于所有业务，易操作，易维护 |
| 用户使用习惯 | 用户使用互联网业务时没有登记真实身份的习惯，实名机制易产生疑虑和抵触 | 用户办理开户业务时要求核实身份，开展业务时用户不感知身份信息，实名制易实施 |

ICP：网络内容提供商




▲图3 基于可信身份标识的安全管理应用

建立网络社会秩序，净化网络环境，避免未成年人遭受不良信息的侵害。

（3）虚拟身份和可信身份绑定，丰富互联网应用。可信身份网络架构要求用户开展各种应用都需携带统一的身份标识，这不利于互联网应用的发展，用户可能也难以接受。通过虚拟身份和可信身份绑定，虚拟身份被用户和ICP在应用层使用，数据传输仍然携带可信身份标识，这种实现一方面延续了现有互联网应用的虚拟和开放性，使得用户仍可使用不同的虚拟身份开展不同的应用，便于应用不断丰富，另一方面数据包携带身份标识也便于网络监管。

## 4 结束语

传统互联网由于IP的名址二义性以及标识用户IP地址不固定的特点，造成了难以识别网络访问主体，使得网络始终处于易攻击、难防控的被动局面。文章通过设计一种可信身份网络架构，实现了名、址彻底分离，用户身份固定，用户和核心网络逻辑隔离，从结构上屏蔽了用户侧直接攻击，提升了网络安全性能。基于固定身份标识开展的安全管理应用，有助于提高攻击源的快速识别能力和溯源效率。可信身份网络架构从技术手段上为网络安全提供保障，同时也为互联网应用的不断发展丰富提供了安全可靠的网络环境。

**参考文献**

[1] 中国互联网络信息中心. 第35次中国互联网络发展状况统计报告[R/OL]. http://cnnic.cn/hlwfzyj/hlwxzbg/
[2] 张再云,魏刚. 网络匿名性问题初探[J]. 重庆社会科学, 2003, 32(2):76–78
[3] 陈剑勇,吴桂华. 身份管理技术及其发展趋势[J]. 电信科学, 2009, 25(2):35–40
[4] 陈周国,蒲石,祝世雄. 匿名网络追踪溯源综述[J]. 计算机研究与发展, 2012, 49(增刊):111–117
[5] 伏晓,蔡圣闻,谢立. 网络安全管理技术研究[J]. 计算机科学, 2009, 36(2):15–19
[6] 高荣林. 网络实名制可行性探讨[J]. 前沿, 2010, 269(15):74–76
[7] 陈兵,邹翔,周国勇. 网络身份管理发展趋势研究[J]. 信息网络安全, 2011, (3):5–8
[8] 史亮,庄毅. 一种定量的网络安全风险评估系统模型[J]. 计算机工程与应用, 2007, 43(18):146–149
[9] 张宏科,苏伟. 新网络体系基础研究——一体化网络与普适服务[J]. 电子学报, 2007, 35(4):593–598
[10] YAN Z, ZHOU H, ZHANG H. A Novel Mobility Management Mechanism Based on an Efficient Locator/ID Separation Scheme[C]// First International Conference on Future Information Networks. USA: IEEE, 2009:11–16. DOI:10.1109/ICFIN.2009.5339610
[11] 吴强,江华,符涛. 移动互联网Naming网络技术发展[J]. 电信科学, 2011, 27(4):73–78
[12] 许东晓,蒋铃鸽. 一种新型的位置标识与身份标识分离方法[J]. 计算机应用与软件, 2010, 27(2):233–236
[13] MOSKOWITZ R, NIKANDER P, JOKELA P, et al. Host Identity Protocol: IETF RFC 5201 [S]. April, 2008
[14] KAFLE V P, OTUSUKL H, INOUE M. An ID/Locator Split Architecture for Future Networks[J]. IEEE Communications Magazine, 2010, 48(2):138–144. DOI:10.1109/MCOM.2010.5402677
[15] 马丁,李丹. 网络"实名认证,网名上网"技术研究[J]. 通信技术, 2014, 47(1):91–96

## 作者简介

**毛玉欣**，中兴通讯股份有限公司高级工程师；主要研究方向为移动互联网、网络安全；有15项发明专利和26篇国际标准提案。

**郝振武**，中兴通讯股份有限公司专家级高工，移动网络和移动多媒体技术国家重点实验室成员；主要研究方向为移动互联网、网络安全；有32项发明专利和30篇国际标准提案。

**江家仁**，中国电信股份有限公司上海研究院高级工程师，移动互联网系统与应用安全国家工程实验室成员；主要研究方向为移动互联网安全技术及安全产品攻防技术。