# 面向可信互联网的 IP 地址管理技术研究 *

马 迪[1,2,3], 毛 伟[1,2], 田 野[1,2], 王 伟[1,2], 王利明[1,2]
(1. 中国互联网络信息中心, 北京 100190; 2. 中国科学院计算机网络信息中心, 北京 100190; 3. 中国科学院研究生院, 北京 100080)

**摘 要**: 作为互联网最重要的基础资源,IP 地址与互联网安全可信有着广泛的联系,包含 IP 地址分配、IP 地址配置以及源地址验证等环节在内的 IP 地址管理工作的研究,是构建可信互联网环境的关键。在构建可信互联网的价值观下,探讨 IP 地址管理层面的研究内容,梳理近年来 IP 地址管理范畴内的研究热点以及相关问题的由来,分析相关的技术方案,并就未来的研究方向进行展望。

**关键词**: 可信互联网; IP 地址管理; IP 地址分配; IP 地址配置; 源地址验证; 互联网审计
**中图分类号**: TP393 **文献标志码**: A **文章编号**: 1001-3695(2012)03-801-07
doi:10.3969/j.issn.1001-3695.2012.03.001

# Survey on technologies of IP address management for trustworthy Internet

MA Di[1,2,3], MAO Wei[1,2], TIAN Ye[1,2], WANG Wei[1,2], WANG Li-ming[1,2]
(1. *China Internet Network Information Center*, *Beijing* 100190, *China*; 2. *Computer Network Information Center*, *Chinese Academy of Sciences*, *Beijing* 100190, *China*; 3. *Graduate University of Chinese Academy of Sciences*, *Beijing* 100080, *China*)

**Abstract**: As the most fundamental resource, IP address has an extensive connection with the trust issue of the Internet. IP address management, including IP address allocation, IP address configuration, source IP address validation and so on, is the key to the establishment of trustworthy Internet. With the establishment of trustworthy Internet as the target, this paper analyzed the origins of different IP address management issues, summarized and evaluated the corresponding countermeasures in history, and envisaged the future research work falling into the category of IP address management.

**Key words**: trustworthy Internet; IP address management; IP address allocation; IP address assignment; source address validation; Internet accountability

## 0 引言

互联网作为当今社会最重要的信息基础设施,极大提高了人类社会生产以及生活的效率,但恶意攻击、网络钓鱼以及垃圾邮件等现象表明互联网并非是足够安全的系统。互联网的不可信因素降低了互联网基础设施的应用价值,成为阻碍互联网进一步蓬勃发展的桎梏。在互联网可信问题日益显著的大背景下,可信网络的概念应运而生,安全性、可生存性和可控性构成了可信网络的基本内涵。可信网络强调设计全新的可信网络安全体系结构,以改变传统打补丁、附加式的安全供给模式[1]。然而,可信网络所描述的价值观和技术目标,要求对当前的互联网络进行重构,无法在短期内部署实现。因此,如何实现当前互联网的安全可信,构建从可用到可信的互联网,成为学术界和工业界的研究热点。

可信互联网的构建是一个复杂的系统工程,由于知识背景和看待问题的角度不同,学术界和工业界所描述互联网可信问题的侧重面也不尽相同。从互联网协议栈的维度进行分析,可信互联网的构建包含:a)物理基础设施层面,包括通信线路、接入系统等;b)基础服务层面,包括 IP 地址管理、域名服务等;c)业务应用层面,包括 WWW 服务、电子邮件、文件传输等。三个层面同时可信才是可信互联网的完整内涵。

在互联网体系结构中,网络层向上承载各种应用,向下屏蔽各式异构物理网络,是互连互通的关键。作为网络层寻址服务的标志,IP 地址是最重要的互联网基础资源。IP 地址管理包含 IP 地址分配、IP 地址配置以及 IP 地址溯源等众多环节,与互联网安全可信有着广泛的联系。因此,IP 地址管理技术的研究是构建可信互联网的关键。

根据网络层不同的通信方式,IP 地址分为单播地址、组播地址(IPv4 称为多播地址)和任播地址(IPv6 特有的地址类型);按照是否可以在互联网上路由的标准,IP 地址又可分为全局可路由地址(public address)和私有地址(private address)[2,3]两类。由于全局可路由的单播地址用来标志单个互

**收稿日期**: 2011-09-25; **修回日期**: 2011-11-11 **基金项目**: 国家发展与改革委员会中国下一代互联网示范工程项目(CNGI-09-03-04); 国家自然科学基金青年科学基金资助项目(61003239)

**作者简介**:马迪(1984-),男,安徽六安人,博士研究生,主要研究方向为互联网资源寻址定位技术、互联网基础资源管理技术(madi@cnnic.cn);毛伟(1968-),男,研究员,博导,博士,主要研究方向为下一代互联网、资源寻址与定位;田野(1979-),男,副研究员,博士,主要研究方向为下一代互联网、无线移动网络安全;王伟(1977-),男,高工,博士,主要研究方向为可信网络及 DNS 协议;王利明(1978-),男,助理研究员,博士,主要研究方向为信息安全、互联网不良信息检测.

联网接入终端,使用最为广泛,对互联网产生的影响最为显著,是 IP 地址空间以及 IP 地址管理内容的主体。本文仅讨论全局可路由的单播地址管理问题,下文在不作特殊说明的情况下,“IP 地址”特指全局可路由的 IP 单播地址。

## 1　IP 地址分配与域间路由安全

传统的域间路由协议 BGP[4](border gateway protocol,边界网关协议)存在很多安全隐患[5],对路由通告内容不加以验证,错误甚至蓄意伪造的路由可达信息可以随意在互联网上传播。具体表现为两种形式:IP 地址前缀劫持和自治域路径信息窜改。前者是指某个自治域发出一个非本自治域内的 IP 地址前缀路由可达通告,导致网络中以该 IP 地址前缀为路由目的的全部或者部分流量被路由至该自治域;后者是指蓄意修改 BGP 报文的自治域路径信息以传播虚假的网络拓扑信息,为后续网络攻击行为作铺垫。

有众多研究针对 BGP 的安全缺陷提出了解决方案:a)以 S-BGP[6]、SoBGP[7]等为代表,旨在协议层面弥补 BGP 的安全缺陷,以抵御 IP 地址前缀劫持和自治域路径信息窜改两种形式的攻击;b)以 DoAV[8]、IPa +[9]以及 RPKI[10]为代表,从完善 IP 地址分配机制的角度来避免 IP 地址前缀劫持。前者涉及 BGP 的协议改进,与 IP 地址管理无直接联系,本文不作讨论;后者从 IP 地址管理的角度出发来保障互联网域间路由安全,是本文要探研讨的重点。

IP 地址前缀和路由源的自治域号(AS 号)的正确映射关系是抵御 IP 地址前缀劫持的关键。互联网注册机构(如亚太互联网络信息中心)天然地拥有 AS 号和 IP 地址的分配信息以及两者的映射关系,但这些信息缺乏统一的数据格式,数据的完整性和一致性也缺乏保障。此外,提供这些信息的查询工具 WHOIS[11]协议没有验证机制,很容易遭受各种类型的攻击。因此,有效地组织 IP 地址分配信息并构建授权信息的验证体系,成为在 IP 地址管理层面抵御 IP 地址前缀劫持的技术路线。

### 1.1　基于 DNS 资源记录的路由源信息发布

基于 DNS 的公共目录服务性质和 DNSSEC[12]安全扩展机制,以 DoAV 和 IPa + 为代表的技术方案通过对 DNS 相关资源记录进行修改,实现了 IP 地址前缀和其路由源映射关系的发布。使用 DNS 反向解析树来反映 IP 地址分配以及授权信息,是这类技术方案的核心思想。

DoAV 建议在 DNS 反向解析树中新增一条子树 bgp. in-addr. arp 来实现特定 IP 地址前缀到其路由源 AS 号的映射。DoAV 设计了一种新的 DNS 资源记录类型“AS 记录”来完成信息的发布。假定 IP 地址前缀 205. 1. 1/24 授权 AS 号为 2914 的自治域为其通告路由可达信息,那么该 IP 地址前缀信息的持有机构,在其维护的 DNS 区文件中添加的资源记录为 1. 1. 205. bgp. in-addr. arpa.　AS 2914 24。基于 DoAV 的设计,边界路由器在使用 BGP 交换路由可达信息时,在 DNS 反向解析树中查询相关 IP 地址前缀的 AS 记录,以验证 BGP 消息中 IP 地址前缀的路由可达信息是否属实。而 DNS 查询数据本身的可信问题交由 DNSSEC 去解决。考虑到新设计的 AS 记录在短期内无法部署,DoAV 建议将相关的路由源信息数据放在 TXT 记录中,但并未给出详细的 TXT 文本表示语法。

作为域间路由安全领域的典型解决方案,S-BGP 尽管设计周密,但需要重新构建一个全球范围的 PKI[13]是其部署的最大障碍。2009 年底,ICANN(the Internet Corporation for Assigned Names and Numbers,互联网名称与数字地址分配机构)对 DNSSEC 实施“根签”,构建了一个基于 DNS 树的全球信任体系。为解决 S-BGP 在部署方面的困难,IPa + 将 DNSSEC 资源记录作为一种轻量级的证书,以完成 IP 地址前缀与其持有实体公钥的关联。与 DoAV 类似,IPa + 也利用了 DNS 中的 IP 地址反向解析树来完成资源的发布,并通过 DNSSEC 中新增的 DS 记录来证明 IP 地址的授权分配关系。例如,ARIN(北美互联网注册机构)持有 IP 地址块 165. 0. 0. 0/8,将其子空间 165. 72. 0. 0/16 分配给 AT&T(美国电话电报公司)。按照 IPa + 的设计,ARIN 通过 DNSSEC 的 DS 资源记录 72. 165. in-addr. arpa DS Hash($KEY_{AT\&T}$)来证明 AT&T 公钥的真实性,以支撑 S-BGP 所设计的路由可达信息签名机制。考虑到 IP 地址前缀的路由源信息不会太过频繁,为提高验证效率,IPa + 采用了周期查询并将查询结果进行缓存的验证机制。

### 1.2　基于 RPKI 的路由源声明

正如 IPa + 提到的那样,构建一个覆盖全球范围的 PKI 是 S-BGP 的最大部署障碍。然而,RPKI(resource PKI)[10]的出现,不仅为 S-BGP 提供了实施基础,更为 IP 地址资源管理提供了一个可信的基础平台。

以 X. 509 证书基本格式为基础,RPKI 通过使用资源证书扩展[14]延伸了 PKI 的功能。资源证书扩展添加了新的 X. 509 值域,用于携带证书持有者所拥有的 IP 地址资源或 AS 号。参照现有的 IP 地址分配体系,上游节点既是其邻接下游节点的资源分配者,也是其邻接下游节点所持有资源证书的颁发者。由于层次化的 IP 地址分配体系, RPKI 为树型信任结构,并采用分布式的 RPKI 资料库存储 IP 地址分配信息。每当有 IP 地址分配信息更新时,RPKI 中的 IP 地址分配者就将新签发的资源证书发布到其管理的 RPKI 资料库中。

基于 RPKI,IP 地址前缀的路由源信息经由一种称为路由源声明的签名项发布,用于说明某个 IP 地址前缀授权给某个 AS 号进行路由可达通告。当需要授权某个 AS 号为特定的 IP 地址前缀通告路由可达信息时,该 IP 地址前缀的持有者使用其资源证书对应的私钥签发一个 EE(endpoint entity)证书,然后再用 EE 证书对应的私钥产生路由源声明签名项。EE 证书中的 IP 地址前缀与路由源声明所表征的 IP 地址前缀一致。完成授权后,IP 地址前缀持有者将相应的路由源声明连同产生该签名项的 EE 证书发布到其管理的 RPKI 资料库中。

依托 RPKI 所提供的可信 IP 地址分配信息以及授权信息,验证者和 RPKI 服务器负责将这些信息推送给边界路由器,供其验证 BGP 消息所携带的 IP 地址前缀路由源信息。验证者(relying party)在全球范围内周期性地下载各个 RPKI 资料库的数据,并通过构造证书路径完成对路由源声明的验证。验证通过后,路由源声明中携带的授权信息被推送到全球各个角落的本地缓存中。一旦收到关于某个 IP 地址前缀的路由可达通告,边界路由器通过 RPKI/router 协议[15]向 RPKI 服务器发起

查询,获得本地缓存的关于该 IP 地址前缀的授权信息,同路由可达通告中携带的路由源信息比较是否一致,并结合本地策略选择是否信任该路由可达通告。

目前,RPKI 在全球范围内引起了广泛关注。全球五大地址注册机构都已提供 RPKI 证书业务,而在技术实现层面,互联网工程任务组(Internet Engineering Task Force, IETF)的 SIDR(Secure Inter-Domain Routing)工作组正在积极推进其标准化工作。

### 1.3　小结

围绕 IP 地址前缀和路由源 AS 号的正确映射关系,或借助 DNSSEC 服务,或在 IP 地址分配体系中构建 PKI,以上技术方案都实现了 IP 地址分配关系和授权信息的真实可信,有效地抵御了 IP 地址前缀劫持。但 DoAV、IPa + 和 RPKI 三者在部署机制、效率以及在域间路由安全的可扩展性方面有所差异,而比较这些差异则是构建可信互联网的重要考量元素。表 1 给出了 DoAV、IPa + 以及 RPKI 三者的比较。

表 1　IP 地址分配与授权信息验证机制比较

| 技术方案 | 认证体系 | 路由器软件升级 | BGP 扩展 | 信息更新机制 | 可扩展性 |
|---|---|---|---|---|---|
| DoAV | DNSSEC | 无 | 无 | 实时查询 | 仅用于验证路由源信息 |
| IPa + | DNSSEC | 无 | 须支持 BGP 签名 | 周期查询 | 仅用于验证路由源信息 |
| RPKI | 专用 PKI | 须支持专门的查询协议 | 无 | 地址分配信息同步推送 | 支持 BGP 安全扩展 |

借助 DNSSEC 所构建的信任链,使用 DNS 反向解析子树来反映 IP 地址分配信息以及授权信息的方法得以实现。这种方法的优势在于充分利用了现有 DNS 基础设施和 DNS 反向解析子树呈现的 IP 地址分配关系,DoAV 和 IPa + 免去了构建额外认证体系的开销,相比 RPKI,部署代价较小。在 IP 地址分配信息以及授权信息获取方面,DoAV 和 IPa + 使用 DNS 的递归解析服务器,RPKI 使用专门的验证实体,后者需要额外部署验证代理业务。此外,RPKI 引入了新的查询协议,需要边界路由器升级软件。

作为一种全新的 IP 地址资源管理机制,RPKI 的部署代价尽管较高,但其通过构建 IP 地址分配以及授权信息的认证体系,为互联网域间路由安全的各种技术方案提供了实施平台。DoAV 和 IPa + 仅仅面向 IP 地址前缀劫持,而 RPKI 通过 BGPSEC[16] 的扩展还可以抵御自治域路径信息窜改。然而,RPKI 未能将 IP 地址分配以及授权领域的所有问题考虑周全,比如在当前 IPv4 地址即将耗尽的背景下,IP 地址交易认证(resource transfer in the global RPKI)会对 RPKI 的运行产生影响,需今后作进一步研究。

## 2　IP 地址配置与接入网安全

在当前的互联网体系结构下,IP 地址是主机在互联网上的身份标志,因此 IP 地址的配置安全直接影响到网络运营商访问控制、计费、溯源等管理技术的实施,是构建可信互联网在接入网层面的主要内容之一。根据不同的配置策略,IP 地址配置主要有静态配置、动态配置以及无状态自动配置[17] 三类。其中,无状态自动配置是 IPv6 内置的新协议,静态和动态配置可以经由主机配置领域的标准化协议 DHCP[18,19](dynamic host configuration protocol,动态主机配置协议)完成。根据配置对象不同的网络层协议,DHCP 分为 DHCPv4[18] 和 DHCPv6[19] 两个版本。在 IPv4 时代,由于 IP 地址稀缺,按需动态的集中式 IP 地址配置方法 DHCPv4 被广泛应用;伴随 IPv6 的到来,IP 地址尽管丰富,但由于集中式的 IP 地址配置机制便于网络管理实体对终端施加控制,DHCPv6 的功能扩展和标准化工作仍然是 IETF 的重点工作之一。考虑到 DHCP 在 IP 地址配置领域的重要地位,本章通过梳理 DHCP 安全领域的技术方案来研讨 IP 地址配置和接入网安全之间的关系。

服务器和客户端是 DHCP 范畴内最基本的两个角色,DHCP 的安全问题主要来自未授权的 DHCP 服务器和未授权的 DHCP 客户端。前者指的是恶意主机伪装成 DHCP 服务器,向用户主机提供错误的 IP 地址等网络参数,导致用户主机无法正常接入互联网;后者是指恶意主机伪造成某个接入网的合法 DHCP 客户端,盗用该网络的 IP 地址、接入带宽等资源。因此,授权和身份验证是 DHCP 安全的核心内容。

### 2.1　DHCP 带外安全技术

由于早期的 DHCP 技术规范中缺乏安全机制,一类以 DHCP snooping[20] 和 UA-DHCP[21] 为代表的技术方案将 IP 地址配置管理和接入控制结合起来,在 DHCP 机制以外寻求 IP 地址配置安全问题的对策。

DHCP snooping 是目前广泛应用的一种基于链路层的安全技术系列,可以用于控制 DHCP 服务器应答报文的来源,以防止网络中伪装或非法的 DHCP 服务器为主机配置 IP 地址及其他网络参数。DHCP snooping 对交换机端口进行区分,将与合法的 DHCP 服务器直接或间接连接的端口设定为信任端口,而将其余端口设置为非信任端口。DHCP snooping 交换机仅转发来自其信任端口的 DHCP 应答消息,保证 DHCP 客户端获取正确的 IP 地址。对于来自非信任端口的 DHCP 服务器应答消息,DHCP snooping 交换机将其丢弃,防止 DHCP 客户端获得错误的 IP 地址。由于 DHCP 服务器一般静态地接入网络,DHCP snooping 能够有效地消除未授权的 DHCP 服务器带来的安全隐患,但 DHCP snooping 缺乏认证机制,未授权的 DHCP 客户端盗用 IP 地址资源的问题无法解决。此外,DHCP snooping 依赖物理端口信息,仅适用于交换式局域网,无法在介质共享式以太网中保障 DHCP 的安全。

UA-DHCP 提出了一种基于“用户名/密码”的 DHCP 客户端认证机制。UA-DHCP 没有改变 DHCP 的核心协议,而是在 DHCP 之外增加了新的认证机制。按照 UA-DHCP 的设计,用户主机首先通过 DHCP 获得 IP 地址,该 IP 地址不能立即使用,仅用于与认证服务器交互完成用户名和密码的验证。验证通过后,网关打开该 IP 地址接入权限,UA-DHCP 周期性检查用户主机的 IP 地址是否处在租约期内,如果过期,则立即要求该 IP 地址对应的用户输入密码加以重新验证;如果验证不能通过,则收回 IP 地址,关闭网关中该 IP 地址的接入权限。本质上,UA-DHCP 先通过 DHCP 配置主机的 IP 地址,然后对用户加以认证来判定是否开放该 IP 地址的接入权限,是抵御未授权的 DHCP 客户端盗用 IP 地址资源的安全技术。然而,UA-DHCP 中基于用户名和密码一致性检查的方法,只能用于一个管理域内,无法适用于漫游主机上的 DHCP 客户端认证。

### 2.2 DHCP 安全扩展技术

带外机制的 DHCP 安全保护机制或依赖接入环境特征,或依赖接入控制策略,没有从根本上改变 DHCP 缺乏身份验证机制的现实,因此在 DHCP 的协议范畴内寻求安全问题的对策,成为学术界和工业界一直以来的热点技术路线,并形成了以 DelayedAuth[22]、DHCP + +[23]、KerbAuth[24]、SigZero[25] 以及 E-DHCP[26] 等为代表的 DHCP 安全扩展研究领域,以解决 DHCP 安全范畴中身份验证的问题。

作为 DHCP 安全扩展技术领域中唯一的 IETF 标准,DelayedAuth 通过在 DHCP 服务器和 DHCP 客户端之间配置预共享密钥完成双向的身份验证,但密钥的预共享机制使得 DelayedAuth 难以灵活且高效地应对站点级网络中大量的配置工作。此外,DelayedAuth 不支持主机的跨域管理,一旦主机变更了接入点,DHCP 服务器和 DHCP 客户端之间的预共享密钥就不再有效。随着海量的移动主机接入互联网,支持跨域身份验证的 DHCP 安全扩展成为后续方案所秉持的基本目标。

与 DelayedAuth 类似,DHCP ++ 同样在 DHCP 服务器和 DHCP 客户端之间实现了基于共享密钥的消息认证码的身份验证机制。较之 DelayedAuth 中密钥的预共享模式,DHCP ++ 通过将密钥协商过程嵌入到 DHCP 的基本消息交互中,实现了验证密钥的自动化管理,支持漫游主机的跨域认证,但 DHCP ++ 的密钥协商机制需要依赖可信第三方为 DHCP 服务器和 DHCP 客户端签发证书。

KerbAuth 是一种基于 Kerberos 在线认证机制[27] 的 DHCP 实体身份验证方法。在 Kerberos 服务器的配合下,KerbAuth 通过 DHCP 的基本消息交互完成密钥在 DHCP 服务器和 DHCP 客户端之间的共享。在 DHCP 服务发现阶段,DHCP 服务器向 DHCP 客户端的家乡 KDC(key distribution center,密钥分发中心)请求与该 DHCP 客户端的共享密钥;在 DHCP 服务确认阶段,DHCP 服务器和 DHCP 客户端使用该密钥认证彼此的身份。KerbAuth 具体的认证运算方法与 DHCP ++ 类似,区别仅在于 DHCP 服务器和 DHCP 客户端之间共享密钥的协商机制。KerbAuth 的实现需要在 DHCP 交互中穿插 Kerberos 协议,在保持 DHCP 状态机一致的要求下,引入了复杂的容错处理开销和管理负担。

由于 DNSSEC 支持在 DNS 的 KEY 记录中存放域名对应的公钥信息,SigZero 以此为基础设计了一种面向主机名的 DHCP 客户端身份验证机制。按照 SigZero 的设计,DHCP 客户端使用 DNS 主机名来标志自己的身份,并使用私钥对发出的 DHCP 消息进行签名,对应的公钥则存放在 DNS 的 KEY 记录中。通过 DNS 查询,DHCP 服务器可以对获取 DHCP 客户端主机名所对应的公钥,进而验证签名。由于验证信息基于 DNS 查询,因此 SigZero 很容易实现。此外,基于 DNS 主机名的身份标志机制可以支持 DHCP 客户端的全互联网漫游身份验证。然而,SigZero 只能用于验证 DHCP 客户端的身份,DHCP 服务器的身份验证仍需要借助其他方法。

基于公钥证书签名机制,E-DHCP 提供了面向双向身份验证的 DHCP 安全扩展方法。E-DHCP 设计中的 DHCP 客户端和 DHCP 服务器均需要经由带外机制获得公钥证书。由于 DHCP 客户端在获得 IP 地址资源之前无法经由互联网构造证书的验证路径,因此,DHCP 客户端必须将 DHCP 服务器的公钥证书添加在本地的信任列表中。利用 DHCP 消息中携带的签名以及带外配置的公钥证书,DHCP 实体的身份验证得以实现。但带外配置信任证书的方式使得 E-DHCP 的 DHCP 服务器身份验证机制只能部署在一个管理域内。

### 2.3 小结

面向 IP 地址配置的安全问题,本章围绕 DHCP 对相关问题的来源和技术方案进行了梳理和分析。这些方案在目标、技术基础、部署难易度以及可扩展性等方面不尽相同,表 2 从不同维度给出了对比。

表 2 DHCP 安全技术方案对比

| 技术方案 | 信任源 | 验证机制 | 安全功能 | 移动性支持 | DHCP 扩展 | 部署要求 |
|---|---|---|---|---|---|---|
| DHCP snooping | 物理网络特征 | 端口绑定 | DHCP 服务器授权认证 | 无 | 无 | 无 |
| UA-DHCP | 带外信任关系 | 用户名/密码 | DHCP 客户端授权认证 | 同一管理域内 | 无 | 需要用户管理模块 |
| Delayed-Auth | 带外信任关系 | 消息认证码 | 双向身份验证 | 同一管理域内 | IETF 技术规范 | 无 |
| DHCP ++ | PKI | 消息认证码 | 双向身份验证 | 跨管理域 | 服务器和客户端行为模式扩展 | 服务器和客户端须支持数字证书 |
| KerbAuth | Kerberos 服务器 | 消息认证码 | 双向身份验证 | 跨管理域 | 服务器和客户端行为模式扩展 | 服务器和客户端须支持 Kerberos |
| SigZero | DNS 权威服务器 | 数字签名 | DHCP 客户端身份验证 | 全互联网漫游 | 签名验证机制 | 无 |
| E-DHCP | PKI | 数字签名 | 双向身份验证 | 同一管理域内 | 签名验证机制 | 服务器和客户端须支持数字证书 |

在安全目标方面,DHCP snooping 和 UA-DHCP 没有触及 DHCP 本身,使用带外机制分别保障了 DHCP 服务器的授权和 DHCP 客户端的授权。而 DelayedAuth、DHCP ++、KerbAuth、SigZero 以及 E-DHCP 等 DHCP 安全扩展机制主要面向 DHCP 本身的安全性,保障 DHCP 实体身份的可验证,没有考虑授权问题。判断 DHCP 服务器和 DHCP 客户端是否是合法的授权实体,需要带外授权信息的辅助。

由于移动接入需求越来越大,跨域管理是 DHCP 安全扩展需要正视的重要问题。DHCP ++、KerbAuth 以及 E-DHCP 可以对移动 DHCP 客户端的身份加以验证,但目前没有一个基于全球信任根的 PKI,这些技术受到其依赖 PKI 有效范围的限制。由于 DNSSEC 已经部署,使用 DNSSEC 作为信任源的 SigZero 对主机移动性的支持是全互联网级的。

在部署层面,DHCP snooping 和 UA-DHCP 仅仅取决于接入网的管理策略,不需要对 DHCP 设备进行改造。而 2.2 节提到的 DHCP 安全扩展技术都需要在协议层面对 DHCP 进行调整。特别是 DHCP ++ 和 KerAuth,两者均在 DHCP 交互流程中嵌入了密钥协商机制,对协议改动较大,是部署的最大障碍。

由于 DHCP 服务器由接入网管理实体部署,管理实体可以利用 DHCP snooping 实现 DHCP 服务侧的可信,思科、华为等设备制造商均支持这项功能。但在 DHCP 客户端认证领域,唯一形成 IETF 技术标准的 DelayedAuth 不支持跨域认证,其余的技术或实现复杂,或仅能支持有限的主机漫游。基于 DNSSEC

的 SigZero 是其中较好的实现方案,但都没有形成相关的技术标准。究其原因,IP 地址配置还同接入网的管理策略密切相关。本章围绕 DHCP 研讨的 IP 地址配置安全机制均未考虑具体的接入认证和计费机制对 DHCP 安全扩展的制约。因此,结合运营商的接入网管理技术以研究面向具体接入环境的安全 IP 地址配置技术是该领域最好的演进方向。此外,随着家庭网络和物联网络的兴起,以及 DHCPv6 开始支持 IP 地址前缀代理[28],IP 地址前缀自动化配置的协议安全将是构建可信互联网范畴内重要的研究内容之一。

## 3　源地址验证

仅仅依赖安全的 IP 地址分配以及配置技术,仍不能完全支撑面向可信互联网的 IP 地址管理工作。由于互联网协议栈的网络层没有实现对数据包源 IP 地址的验证,源 IP 地址可以被随意伪造,作为实施网络攻击的前奏。为了弥补网络层协议设计的缺陷,源地址验证技术应运而生。根据验证机制部署的位置不同,源地址验证技术分为接入网验证、自治域间验证以及端到端验证。

### 3.1　接入网源地址验证

接入网源地址验证技术利用数据包源地址和其转发路径的特定物理信息以及逻辑信息的绑定关系进行过滤。Ingress filtering[29]是一个基于路由器中存储数据结构的轻量级过滤方案,路由器或者防火墙负责检查来自这个网络数据包的源 IP 地址是否属于这个网络,它可以使伪造源 IP 地址的数据包不能离开攻击者所属的子网,但无法抵御子网内的源地址伪造。

为防止子网内的源地址伪造,SPINACH[30,31]将 IP 地址和 MAC 地址的绑定关系注册到转发设备上,但 MAC 地址可以被用户修改,这种方法的脆弱性显而易见。SPINACH 的作者进一步提出了一种面向交换式局域网的解决方案,以利用端口信息进行源地址验证。使用 IP 地址和交换机端口绑定关系完成源地址验证的做法很快就体现在了后续的解决方案中。历经发展,Ethane[32]是目前较为成熟的方案,但 Ethane 这种基于交换式局域网的设计仍旧没有彻底解决共享式以太网的源地址验证问题。

IPv6 的出现为接入网源地址验证提供了新的技术基础。清华大学的研究人员提出了一种使用 IPv6 扩展包头携带验证信息的源地址验证方法[33]。在该方法中,接入主机和接入网关之间共享密钥。主机在发送数据包之前,使用其与接入网关之间共享的密钥对数据包载荷进行哈希运算,并将运算结果携带在新设计的 IPv6 验证包头中供接入网关验证。然而,该方法并未对如何在接入主机和验证网关之间共享密钥进行细致的设计。CSAA[34]利用 CGA[35]的自验证特性提出了一种具体的共享密钥分发机制。

使用共享密钥进行载荷哈希运算的验证机制可以实现高粒度的源 IP 地址验证,且不依赖于具体的接入环境特征,但密钥共享仍然受制于不同的接入控制协议。如何在不同的接入控制协议中捎带完成共享密钥在接入主机和验证网关之间的高效配置,尚有很多值得研究的内容。

### 3.2　自治域间源地址验证

依托本文第 1 章研讨的域间路由安全技术,以 SAVE[36]、SPM[37]和 Passport[38,39]等为代表的域间源地址验证技术流派实现了 IP 地址前缀粒度的源地址验证。

在自治域的边界路由器上,SAVE 对 IP 地址前缀与接收到该前缀的路由通告消息的接口建立关联。SAVE 的实现依赖边界路由器之间相互交换域间路由信息,使得边界路由器涉及到大量的、可认证的数据交换。SAVE 的复杂性比较高,可能成为 DoS 攻击的潜在对象。

与 SAVE 利用路由信息不同,SPM 引入了一种轻量级签名机制在自治域对之间实现源地址验证。根据 SPM 的设计,当数据包离开源自治域时,自治域的边界路由器将为其添加一个基于源—目的自治域对的签名,以供目的自治域的边界路由器验证。SPM 中所谓的签名没有采用任何加密技术,而是在数据包中携带源—目的地址对、源—目的 IP 地址前缀对或者源—目的 AS 号对的共享秘密,该秘密为一个常数。SPM 的安全性基于骨干网报文难以被窃听的前提,但由于共享秘密以明文形式携带在数据包中,数据包在穿越自治域时,很可能被中间人窃听。

针对 SPM 中共享秘密容易被窃听的缺陷,Passport 提出了一种基于数字签名的源地址验证方法。源地址所在自治域需要与数据包转发路径上的各个自治域分别共享密钥,并使用这些共享密钥分别产生签名供数据包沿途的各个自治域边界路由器验证。在数据包被路由至目的主机之前,一旦出现签名验证不正确或不存在的情况,该数据包就将被丢弃。较之 SAVE 和 SPM,Passport 最鲜明的特点是引入了密码学的签名技术,此举使得域间路由的数据包负荷增大,一旦数据包需要途径多个自治域,源自治域为数据包添加的签名将会很长,对骨干网的带宽消耗明显。

### 3.3　端到端的主机级源地址验证

以上提到的若干源地址验证技术均在数据包的传输路径部署实施,对终端主机透明。尽管这些方案免去了数据包接收者的验证负担,但某些高安全要求的应用需要数据包的接收者亲自验证源地址。从源 IP 地址缺乏认证的根本出发,IPSec[40~42]设计了新的 IP 数据包扩展头,使其携带目的主机和源主机之间基于共享密钥的哈希签名。共享密钥以及验证策略等 IPSec 安全参数,可由管理员分别在通信双方的主机上手工配置,还可以使用专门的密钥交换协议[43]来完成端到端的协商。

IPSec 在互联网的完整部署依赖于是否存在一个可信的并且能够处理海量用户证书的 PKI。IPSec 的管理也较为复杂,容易出现相关参数配置的错误配置。总之,证书管理和操作管理是 IPSec 实践和推广中最大的难题。

### 3.4　小结

由于互联网体系结构设计上的缺陷,源地址验证是一个复杂的系统工程。为了有效地部署源地址验证机制,清华大学的研究人员设计了互联网源地址验证的整体框架[44],对各种源地址验证技术进行了整合,并在 IETF 发起成立了 SAVI(source address validation improvements)工作组,以推进相关技术细节的标准化。由于互联网边缘网络在物理特征、接入控制技术、资源分配机制以及管理策略上的巨大差异,源地址验证技术必须同具体接入环境结合,随着互联网由 IPv4 向 IPv6 演进,研究

面向 IPv6 特征,特别是其地址结构特征的源地址验证技术,如之前提到的 CSAA,将是今后该领域的演进方向之一。

纵览源地址验证技术的发展,验证机制都是对目前互联网体系结构下网络层工作机制的补充,依赖部署政策和网络运营策略,没有在根本上实现数据包源 IP 地址的真实可信。对于这一技术发展瓶颈,本文下一章提到的互联网审计研究领域给予了足够的关注和解决手段。

## 4 面向 IP 地址的互联网审计

围绕 IP 地址管理的不同环节,上文对相关的技术进行了梳理和分析。这些技术尽管在基础资源层面为构建从可用到可信的互联网提供了有力的支撑,但这些技术或是已有技术的改进,或是对互联网体系结构的修补,没有触及当前互联网体系结构的内核,致使互联网的基础资源管理和协议簇越来越复杂。鉴于网络层在互联网协议栈中的重要地位以及上文在综述 IP 地址管理技术问题时提到的困难乃至瓶颈,工业界和学术界越来越来深刻地认识到互联网体系结构研究对于可信互联网的重要性。IP 地址分配、配置以及验证等环节的安全技术研究直接推动了面向 IP 地址的互联网审计的问世。

由于缺乏内在的审计机制,互联网并非一个足够安全的基础通信平台。审计(accountability)是指准确地将特定的行为同产生该行为的实体身份关联起来,并实施有效的问责。由于 IP 地址独立于互联网上层应用的特点,面向 IP 地址的互联网审计成为近年来一个新兴的研究领域。AIP[45] 和 BAFI[46] 是该领域最具代表性的技术方案。

在源地址伪造之外,很多互联网的合法运行机制导致 IP 地址溯源困难,IP 地址审计难以实现。例如,DHCP 的使用导致同一 IP 地址先后被分配给不同主机使用,漫游主机的 IP 地址随着接入点的变更而变化。因此,在协议上实现 IP 地址可验证以及在资源管理上实现 IP 地址易溯源,成为面向 IP 地址的互联网审计领域的基本出发点。

通过对网络层协议进行重构,AIP 使用扁平化结构的自验证 IP 地址取代了层次化结构的聚合式 IP 地址。AIP 假设互联网由若干管理上独立但彼此互连的网络组成,每个网络又由若干个审计域组成。每个审计域将其公钥的哈希作为自己的标志符,审计域之中的终端同样使用自己的公钥哈希值作为身份标志符。审计域标志符和终端标志符共同组成了一个完整的 IP 地址,这种设计成功地实现了“身份”和“位置”两个语义在 IP 地址结构内的区分。基于新的 IP 地址结构,AIP 进一步设计了网络层内置的源地址验证协议、域间路由安全机制并讨论了新的网络层协议下的可扩展路由问题。源地址验证和 IP 流量控制构成了 AIP 互联网审计机制的基本内涵。

在 AIP 之后,BAFI[46] 也提出了一种互联网审计方法。BAFI 首先抽象出了一种可以区分“身份”和“位置”两个语义的 IP 地址。在此前提下,BAFI 基于陷门哈希函数签名方法实现了一种轻量级的网络层消息签名机制[47],用以验证数据包发送源的非否认性和数据包载荷的完整性。在源地址验证的基础上,BAFI 进一步提出了客户端票据的概念。客户端票据包含了客户端和服务器双方的身份信息、服务端主机所在的自治域号码以及有效时间等信息,可以协助服务器端主机方便地进行流量控制。基于陷门哈希函数的签名机制还使得 BAFI 方便地建立起了面向 IP 地址的互联网信誉评价系统。按照 BAFI 的观点,源地址验证、流量控制和信誉评价系统构成了互联网审计最基本的三个要素。BAFI 的审计仅仅面向客户端,强调对通信发起实体的审计,没有讨论互联网控制实体如数据转发设备的审计问题。正如 AIP 在论述互联网审计概念时提到的那样,完整的互联网审计应当包含源实体审计(source accountability)和控制实体审计(control-plane accountability)。

互联网审计的概念兴起不久,相关研究也较少,但互联网审计是构建 从可用到可信的互联网的关键,是可信互联网研究在 IP 地址资源管理领域的自然延伸。当前的研究反映出这样一个事实:在网络层实现互联网接入实体身份标志和位置标志的解耦,是实现互联网审计的必要条件,但在当前的互联网体系结构下难以实现。无论 AIP 还是 BAFI,都是对下一代互联网互连互通层次标志设计的前瞻性研究,提出的解决方案无法与现有互联网 IP 地址结构或使用方式兼容,但 IPv6 地址的广泛使用在即,AIP 和 BAFI 所折射的研究思想将有助于挖掘 IPv6 互联网提供审计的潜力。

## 5 结束语

目前,全球互联网数字分配机构(IANA)正式宣布已经将 IPv4 地址库剩余的五个 A 地址,平均分配给包括亚太区互联网络信息中心在内的五个地区性互联网注册管理机构,标志全球现有的 IPv4 地址资源已经分配完毕,IPv6 地址规划时代正式到来。IPv6 的兴起不仅源于 IPv4 地址空间的局限,尽可能地弥补 IPv4 时代互联网安全上暴露的缺陷,也是 IETF 设计 IPv6 地址时的重要考量。

IPv6 是网络技术史上的一次重要升级,IPv6 在协议以及 IP 地址结构层面的特征为面向可信互联网的 IP 地址管理技术研究带来了机遇。如何解决 IPv6 地址管理中的诸多问题,在 IPv4 到 IPv6 的演进过程中构建从可用到可信的互联网,将是互联网社区重要的研究内容之一。

**参考文献:**


[1] 林闯,彭雪海. 可信网络研究[J]. 计算机学报,2005,28(5):751-758.

[2] REKHTER Y, MOSKOWITZ B, KARRENBERG D, *et al*. RFC 1918, Address allocation for private Internets [S]. Fremont: IETF, 1996.

[3] HINDEN R, HABERMAN B. RFC 4193, Unique local IPv6 unicast addresses [S]. Fremont: IETF, 2005.

[4] REKHTER Y, LI T, HARES S. RFC 4271, A border gateway protocol 4 (BGP-4) [S]. Fremont: IETF, 2006.

[5] MURPHY S. RFC 4272, BGP security vulnerabilities analysis [S]. Fremont: IETF, 2006.

[6] KENT S, LYNN C, MIKKELSON J, *et al*. Secure border gateway protocol (S-BGP): real world performance and deployment issues [C]//Proc of the 7th Annual Symposium on Network and Distributed System Security. [S.1.]: The Internet Society, 2000: 1-14.

[7] WHITE R. Securing BGP through secure origin BGP(SOBGP) [J]. Business Communications Review, 2003, 33(5): 15-22.

[8] BATES T, BUSH R, LI T, *et al*. Draft-bates-bgp4-nlri-orig-verif-00, DNS-based NLRI origin AS verification in BGP [R]. Fremont: IETF,

1998.

[9] YANG Xiao-wei, LIU Xin. Interent protocol made accountable [C]//Proc of the 8th ACM SIGCOMM Workshop on Hot Topics in Network. 2009.

[10] HUSTON G, MICHAELSON G, KENT S. Resource certification: a public key infrastructure for IP addresses and AS's [C]//Proc of IEEE GLOBECOM Workshops. Washington DC: IEEE Computer Society, 2009: 1-6.

[11] DAIGLE L. RFC 3912, Whois protocol specification [S]. Fremont: IETF, 2004.

[12] ARENDS R, AUSTEIN R, LARSON M, *et al*. RFC 4034, Resource records for the DNS security extensions[S]. Fremont: IETF, 2005.

[13] CHOKHANI S, FORD W, SABETT R, *et al*. RFC 3647, Internet X.509 public key infrastructure certificate policy and certification practices framework [S]. Fremont: IETF, 2003.

[14] LYNN C, KENT S , SEO K. RFC 3779, X.509 extensions for IP addresses and AS identifiers [S]. Fremont: IETF, 2004.

[15] BUSH R, AUSTEIN R. Draft-ietf-sidr-rpki-rtr-16, the RPKI/router protocol[R]. Fremont: IETF, 2011.

[16] LEPINSKI M, TURNER S. Draft-ietf-sidr-bgpsec-overview-00, an overview ofBGPSEC[R]. Fremont: IETF, 2011.

[17] THOMSON S, NARTEN T, JINMEI T. RFC 4862, IPv6 stateless address autoconfiguration[S]. Fremont: IETF, 2007.

[18] DROMS R. RFC 2131, Dynamic host configuration protocol[S]. Fremont: IETF, 1997.

[19] DROMS R, BOUND J, VOLZ B, *et al*. RFC 3315, Dynamic host configuration protocol for IPv6 [S]. Fremont: IETF, 2003.

[20] Cisco Systems Inc. Understanding and configuring DHCP snooping [R/OL]. http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.1/12ew/configuration/guide/dhcp.pdf.

[21] KOMORI T, SAITO T. The secure DHCP system with user authentication[C]//Proc of the 27th Annual IEEE Conference on Local Computer Networks. Washington DC: IEEE Computer Society, 2002: 123-131.

[22] DROMS R, ARBAUGH W. RFC 3118, Authentication for DHCP messages[S]. Fremont: IETF, 2001.

[23] ARBAUGH W A, KEROMYTIS A D, SMITH J M. DHCP++: applying an efficient implementation method for fail-stop cryptographic protocols [C]// Proc of Global Telecommunications Conference. [S.l.]: IEEE Press, 1998: 59-65.

[24] HORNSTEIN K, LEMON T, *et al*. Draft-hornstein-dhc-kerbauth-06, DHCP authentication via Kerberos V[R]. Fremont: IETF, 2001.

[25] LEMON T, RICHARDSON M. Draft-ietf-dhc-auth-sigzero-00, DHCP RSA/DSA authentication using DNS KEY records [R]. Fremont: IETF, 2003.

[26] DEMERJIAN J, SERHROUCHNI A. DHCP authentication using certificates [C]//IFIP International Federation for Information Processing, vol 147. Berlin: Springer-Verlag, 2004: 456-472.

[27] KOHL J, NEUMAN C. RFC 1510, The Kerberos network authentication service (v5) [S]. Fremont: IETF, 1993.

[28] TROAN O, DROMS R. RFC 3633, IPv6 prefix options for DHCPv6 [S]. Fremont: IETF, 2003.

[29] FERGUSON P, SENIE D. RFC 2267, Network ingress filtering: defeating denial of service attacks which employ IP source address spoofing [S]. Fremont: IETF, 2000.

[30] POGER E, BAKER M. Secure public Internet access handler (SPINACH) [C]//Proc of USENIX Symposium on Internet Technologies and Systems. Berkeley: USENIX Association, 1997: 11.

[31] APPENZELLER G, ROUSSOPOULOS M, BAKER M. User-friendly access control for public network ports [C]//Proc of the 18th Annual Joint Conference on IEEE Computer and Communications Societies. New York: IEEE Press, 1999: 699-707.

[32] CASADO M, FREEDMAN M J, PETTIT J, *et al*. Ethane: taking control of the enterprise[C]//Proc of Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications. New York: ACM Press, 2007: 1-12.

[33] XIE Li-zhong, BI Jun, WU Jian-pin. An authentication based source address spoofing prevention method deployed in IPv6 edge network [C]//Proc of the 7th International Conference on Computational Science. Berlin: Springer-Verlag, 2007: 801-808.

[34] YAO Guang, BI Jun. A CGA based IP source address authentication method in IPv6 access network [C]//Proc of the 33rd IEEE Conference on Local Computer Networks. [S.l.]: IEEE Press, 2008: 534-535.

[35] AURA T. RFC 3972, Cryptographically generated addresses (CGA) [S]. Fremont: IETF, 2005.

[36] LI Jun, MIRKOVIC J, WANG Meng-qiu, *et al*. SAVE: source address validity enforcement protocol [C]// Proc of the 21st Annual Joint Conference on IEEE Computer and Communications Societies. New York: IEEE Press, 2002: 1557-1566.

[37] BREMLER-BARR A, LEVY H. Spoofing prevention method [C]// Proc of the 24th Annual Joint Conference on IEEE Computer and Communications Societies. New York: IEEE Press, 2005: 536-547.

[38] LIU Xin, YANG Xiao-wei, WETHERALL D, *et al*. Efficient and secure source authentication with packet passports [C]//Proc of the 2nd Conference on Steps to Reducing Traffic on the Internet. Berkeley: USENIX Association, 2006: 2.

[39] LIU Xin, LI Ang, YNAG Xiao-wei, *et al*. Passport: secure and adoptable source authentication[C]//Proc of the 5th USENIX Symposium on Networked Systems Design and Implementation. Berkeley: USENIX Association, 2008: 365-378.

[40] KENT S, SEO K. RFC 4301, Security architecture for the Internet protocol [S]. Fremont: IETF, 2005.

[41] KENT S. RFC 4302, IP authentication header[S]. Fremont: IETF, 2005.

[42] KENT S. RFC 4303, IP encapsulating security payload(ESP)[S]. Fremont: IETF, 2005.

[43] KAUFMAN C, HOFFMAN P, NIR Y, *et al*. RFC 5996, Internet key exchange protocol version 2 (IKEv2) [S]. Fremont: IETF, 2010.

[44] WU Jian-ping, REN Gang, LI Xing. Source address validation: architecture and protocol design[C]//Proc of IEEE International Conference on Network Protocols. [S.l.]: IEEE Press, 2007: 276-283.

[45] ANDERSEN D, BALAKRISHNAN H, FEAMSTER N, *et al*. Accountable Internet protocol (AIP) [C]//Proc of ACM SIGCOMM Conference on Data Communication. New York: ACM Press, 2008: 339-350.

[46] MIRKOVIC J, REIHER P. Building accountability into the future Internet [C]//Proc of the 4th Workshop on Secure Network Protocols. [S.l.]: IEEE Press, 2008: 45-51.

[47] SHAMIR A, TAUMAN Y. Improved online/offline signature schemes [C]//Proc of the 21st Annual International Cryptology Conference on Advances in Cryptology. London: Springer-Verlag, 2001: 355-367.