软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2014,25(1):78−97 [doi: 10.13328/j.cnki.jos.004509]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

互联网地址安全体系与关键技术*

徐 恪[1,2], 朱 亮[1,2], 朱 敏[1,2]

[1](清华信息科学与技术国家实验室(清华大学),北京 100084)

[2](清华大学 计算机科学与技术系,北京 100084)

通讯作者: 徐恪, E-mail: xuke@mail.tsinghua.edu.cn, http://www.tsinghua.edu.cn

摘 要: 当前,互联网体系结构不具备地址真实性验证机制,源地址伪造与路由地址前缀欺骗造成了极大危害.解决地址安全问题、构建真实可信的互联网环境,已成为亟待解决的重要课题.地址的真实性是互联网可信的基础和前提.针对这些问题,研究者们从不同角度提出了很多解决方案.首先,该文介绍了地址的概念及其欺骗现状,分析了地址安全的含义,并从研究体系、实现机制以及关键技术这 3 个维度,对地址安全研究思路进行了归纳分析.然后,对典型地址安全方案的性能指标进行了总结.最后,给出了一个地址与标识通用实验管理平台的设想,基于该平台,可以为不同的地址标识方案提供统一的部署实验环境.

关键词: 地址欺骗;前缀劫持;地址安全;地址认证;通用地址平台

中图法分类号: TP393 **文献标识码**: A

中文引用格式: 徐恪,朱亮,朱敏.互联网地址安全体系与关键技术.软件学报,2014,25(1):78−97. http://www.jos.org.cn/1000-9825/4509.htm

英文引用格式: Xu K, Zhu L, Zhu M. Architecture and key technologies of internet address security. Ruan Jian Xue Bao/Journal of Software, 2014,25(1):78−97 (in Chinese). http://www.jos.org.cn/1000-9825/4509.htm

Architecture and Key Technologies of Internet Address Security

XU Ke[1,2], ZHU Liang[1,2], ZHU Min[1,2]

[1](Tsinghua National Laboratory for Information Science and Technology (Tsinghua University), Beijing 100084, China)

[2](Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China)

Corresponding author: XU Ke, E-mail: xuke@mail.tsinghua.edu.cn, http://www.tsinghua.edu.cn

Abstract: Forged source address and routing address prefix hijacking have caused great threats since there are no source address validation mechanisms on the current Internet. Solving the address security problem and constructing a reliable Internet environment have become a critical issue. The foundation of a trustworthy Internet is the authenticated IP addresses. Therefore, researchers have proposed many solutions from different perspectives on these problems. This paper first introduces the notion of address and the current situation of address spoofing, then gives an analysis to the meaning of the address security. The paper analyzes and compares these security solutions in three dimensions: The architecture, the mechanism and the key technical means. Their performances are also summarized and evaluated. Finally, the study provides a proposal of constructing a general experimental platform for network addresses which enables different address schemes to be deployed and experimented.

Key words: address spoofing; prefix hijacking; address security; address authentication; general address platform

1 引 言

互联网已成为重要的信息基础设施,E-mail、社交网络、电子商务到网上银行等各种活动,都需依托互联网

* 基金项目: 国家自然科学基金(61170292); 国家重点基础研究发展计划(973)(2009CB320501, 2012CB315803); 国家科技重大专项(2012ZX03005001-001); 国家高技术研究发展计划(863)(2013AA013302); 国家科技支撑计划(2011BAK08B05-02, 2012BAH01B01)

收稿时间: 2013-01-08; 修改时间: 2013-07-30; 定稿时间: 2013-10-11; jos 在线出版时间: 2013-11-21

CNKI 网络优先出版: 2013-11-21 12:38, http://www.cnki.net/kcms/detail/11.2560.TP.20131121.1238.001.html

进行.然而,当前互联网的安全机制较为薄弱,系统性不强,各种欺骗、隐私窃取等恶意攻击泛滥,安全问题越来越引起人们的关注,互联网的可信任性已影响到国家经济发展以及社会的和谐稳定.在现有的互联网体系结构中,地址同时兼具身份与位置双重属性,这种语义过载的特性造成了大量基于地址欺骗的攻击,不仅严重扰乱互联网秩序,同时隐藏了肇事者的身份以致很难溯源追查.因此可以说,地址的安全性是构建可信任互联网的基础.但当前,互联网并不具备地址真实性验证的内在机制,地址的安全可信已成为亟待解决的重要问题之一.由Clark 等人主导、美国多所高校联合研究的项目 NewArch[1]明确指出:包括地址验证在内的身份验证体系,对下一代互联网安全具有关键意义.为了解互联网地址安全的研究现状,本文从研究体系、实现机制以及关键技术这 3 个维度对目前的地址安全技术进行了归纳研究,并在深入分析的基础上,对它们的地址欺骗防御能力、可部署性以及开销等指标进行了对比与评估.

1.1 地址概念

Shoch 最早给出了关于地址的定义——“An address indicates where it is”[2],该定义简单且容易被理解,类似于我们日常生活中的邮政系统,即地址标识了主体的地理位置.2011 年,Woojik 等人为了分析名字、地址、身份标识、定位标识这四者的关系,给地址赋予了一个新的定义——“An address denotes position to where an entity can be placed (or attached)”[3],并认为:地址在能够唯一标识主体的情况下,可以被作为身份标识使用.而在当前互联网体系结构中,IP 地址的语义至少包括身份(identifier)和位置(locator)这两种属性[4],其中,身份属性用来标识通信对端,而定位属性代表拓扑位置,是路由寻址的基础.也就是说,具有持久性的身份标识与动态的拓扑位置其实是绑定在一起的,这难免会带来一系列的管理和安全问题.为了解决这些问题,研究者们开始从地址本身的构造方式、结构特征以及路由寻址协议着手进行创新性改造,也提出了很多替代传统 IP 地址的方案.由于实现思想及技术手段的区别,这些方案中的地址分别聚合了不尽相同的语义特征和属性空间.本文所论述的地址可以定义为:以某种方式产生,兼具位置标识、身份标识以及结构、安全、可扩展等多重属性的网络实体标签.而地址的安全主要是指地址属性中身份和位置属性的可信可控.

1.2 地址欺骗

当前的互联网变得越来越庞大而复杂,已不具备通信双方互相信任的前提.Steiner 的那副卡通画“On the Internet, nobody knows you are a dog”[5]非常形象地说明了互联网中用户的匿名性.上一节中提到的 IP 地址兼具身份和定位的语义过载特性带来了极大的安全威胁,甚至阻碍了互联网体系结构的演进发展.当前,互联网中的网络设备仅根据报文中的目标 IP 地址进行寻址转发,并不对源地址进行验证;核心协议 BGP(border gateway protocol)缺乏路由信息认证机制,路由安全,尤其是地址前缀宣告的真实性面临极大的威胁.鉴于此,本文讨论的地址欺骗主要体现在以下两个方面:

1) 源地址欺骗:产生原因在于用户可以随意伪造报文中的源 IP 地址以隐藏身份,而数据平面无法验证一个节点是否拥有其所声明的源地址.互联网中大量的网络攻击(如 Dos/DDos[6],flooding attack[7],smurf[8]攻击等)大都借助了源地址欺骗技术,使得追溯定位变得极为困难;
2) 地址前缀欺骗:前缀劫持是 BGP 面临的最主要的威胁[9],产生的根本原因在于互联网体系结构的控制平面缺少验证 AS 是否授权通告某 IP 前缀的安全机制,恶意 AS 可以对外宣告一个不属于自身的 IP 地址前缀以劫持网络流量,进行监听、篡改等恶意行为,文献[10,11]分别从技术和经济的角度对前缀劫持进行了深入分析.

结合以上两类安全威胁,攻击者可以伪装成他人的身份进行非法操作,或是劫持路由地址前缀以改变分组流向,从而达到不可告人的目的,我们称这种行为为地址欺骗.

2005 年,MIT ANA 成立了 Spoofer Project 研究小组[12],通过全球范围内的测试主机向服务器发送源地址欺骗分组,来探测这些主机是否存在地址欺骗的能力,并用以进行不同欺骗粒度的统计.2012 年 11 月 18 日发布的研究结果表明(如图 1 所示[13]):有 17.3%IP 地址表示的主机、14.3%网络前缀以及 23.3%的自治系统中的攻击者可以进行 IP 地址欺骗攻击(spoofable).这里的 spoofable 指的是至少可以成功伪造一个源地址,也就是说,实际可

以伪造的 IP 源地址将远远高于 17.3%.虽然相比之前的数据,unspoofable 的端系统(即能够被防御机制有效拦截的)数量大幅增加[14],但可执行地址欺骗的主机仍然占据着相当可观的比例.

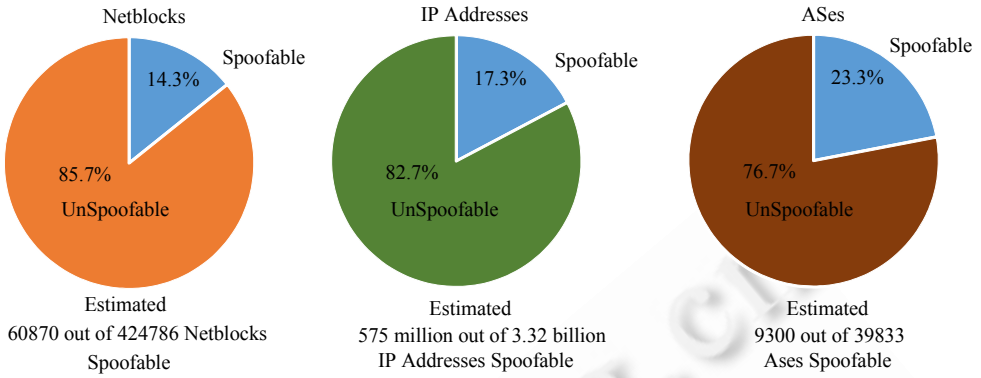


Fig.1 Current situation of IP spoofing (2012-11)[13]

图 1 IP 地址欺骗现状(2012-11)[13]

近年来,地址前缀劫持事件也是层出不穷,给互联网的正常运行带来了极大的危害.其中比较著名的是 2008 年巴基斯坦的恶意劫持事件[15]:为了对国内用户屏蔽 YouTube 网站,巴基斯坦电信管理局在本国范围内宣告了伪造的地址前缀,但由于配置错误,导致该非法前缀向全球蔓延,从而造成大量用户对 YouTube 的访问中断.这表明:IP 地址欺骗仍然是互联网中一个巨大的安全漏洞,必须引起人们的足够关注[16].

1.3 互联网地址安全

从上节中对地址欺骗的分析可知,互联网地址安全应包括源地址安全以及路由前缀安全两个方面:伪造的源地址隐藏了攻击者的身份,被劫持的地址前缀导致网络流量被重定位到非法目的位置.然而,当前互联网体系结构的数据平面和控制平面中都不具备地址真实性认证的安全机制.可以说,确保互联网地址身份及其位置属性的真实可信,已成为下一代互联网研究中重要的技术挑战[17].

本文所论述的地址安全可以概括为(如图 2 所示):通过一定的安全手段,保证地址身份标识的唯一性以及路由位置的真实性;确保地址(前缀)来自于授权使用方,在分配及使用过程中不被篡改、伪造;对于非授权的地址(前缀)应能及时检测或过滤,从而为互联网安全可信提供良好的基础.

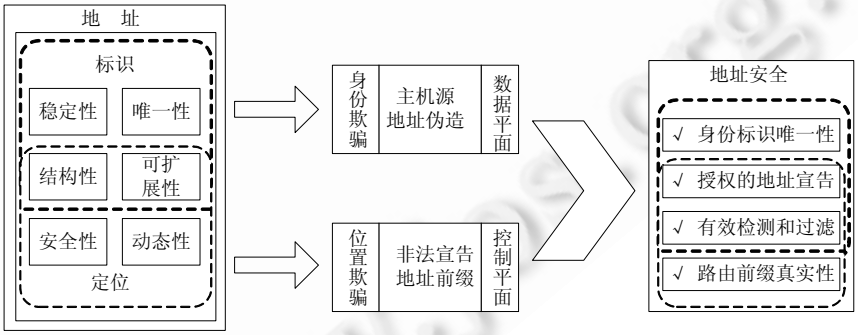


Fig.2 Definition of Internet address security

图 2 互联网地址安全概念

2 互联网地址安全的研究体系

自 1989 年 Bellovin 指出基于地址欺骗是存在于互联网中一种极具威胁的安全问题[18]以来,地址安全研究不断推陈出新.一个优秀的方案应能在保证地址安全的同时还具有易于部署、开销低等特性,这将是地址安全

研究面临的一个长期挑战.

地址和路由系统是当前互联网体系结构的核心,要对它们做出革新无疑是非常困难的.因此,早期的研究集中在体系结构缺陷的修补上,并不对地址或路由协议作本质革新.随着研究的不断深入,研究工作开始从地址的语义特征以及协议的扩展着手,以建立一套完整的路由寻址协议乃至从体系结构为出发点来解决地址安全问题.借鉴于互联网体系结构研究思路的划分,本文从是否对地址或路由协议进行扩展或革新的层面上,将地址安全研究归为"改良型"和"革新型"两类研究体系.

2.1 "改良型"研究思路

互联网几十年来取得了巨大成功,IP 地址和域间路由协议 BGP 作为体系结构的核心基础,证明了其强大的适应性和稳定性,轻易地变革将会导致设计和部署上的巨大开销[19].鉴于此,"改良型"的研究思路采用"增量式修补"策略,在保证现有地址体系和路由协议稳定的基础上,通过增加检测机制以保障地址安全.这类检测方案的基本思想是:正常情况下,网络中的分组流向、路由状态等特征应当是稳定的,检测机制通过在主机、路由器或第三方进行监测与地址相关的网络特征,若出现异常,则怀疑发生了地址欺骗.如:伪造源地址的报文进入路由器的接口可能会发生变化;而地址前缀劫持常会被检测到多个 AS 宣告相同前缀的异常现象(MOAS 冲突)[20].

2.2 "革新型"研究思路

这类研究认为修补的方法缺少设计的指导原则[21],并且不能从根本上解决地址安全问题,只是一种事后的补救策略.因此,研究者们开始从协议的改进或更新入手来解决问题,研究的重点转向了在地址系统和路由协议中绑定安全机制,使用密码学的方法实现源地址的认证.主要研究工作包括创建能够自我验证的地址以及对源 AS 授权认证两方面.另外,为了解决移动性及路由可扩展性问题,业界提出了很多 IP 地址身份和位置标识分离(ID/LOCATOR split)[22,23]的方案.虽然其初衷是为了建立一套基于身份、定位功能分离的新型互联网体系结构,但其解决了 IP 语义过载这一根本问题,因此对互联网的地址安全也具有十分重要的意义.

2.3 地址安全研究思路分析

"改良型"方案具有较强的部署能力,但不能从源头上避免地址欺骗,而且大量补丁势必造成地址以及路由系统性能的下降;"革新型"的研究思路试图从根本上保证地址安全,但其所带来的开销以及实际部署能力不容乐观.图 3 展示了互联网地址安全研究体系、机制、技术手段以及三者之间的隶属关系.

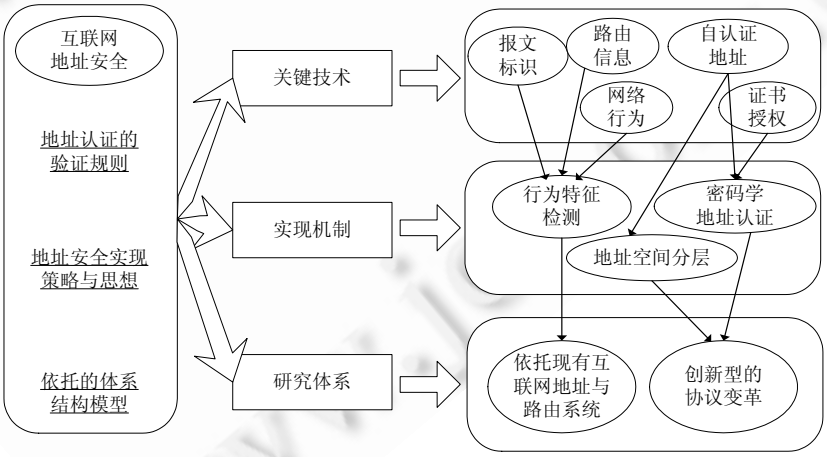


Fig.3 Architectures, mechanisms and technologies of address security

图 3 地址安全研究体系、机制与技术

3 互联网地址安全的实现机制

基于密码学的源认证机制能够对地址(前缀)宣告源进行授权认证,是一种欺骗避免机制,但其巨大开销带来的部署难题一直遭受质疑;从实际可部署的角度出发,基于行为特征检测的安全机制受到越来越多研究者的关注;而地址空间分层机制则重新定义了地址的基本语义和属性,对地址安全具有重要的意义.

3.1 基于密码学的源认证机制

无论是端系统的源地址欺骗还是地址前缀劫持,其根本原因都在于无法鉴别源的真实性,即无法验证源主机(AS)是否拥有其宣告地址(前缀)的授权.源认证是一种确认地址所有权的方法,基本思想是:在地址构造或BGP 协议中使用密码技术进行源真实性鉴别,从而在根本上避免地址欺骗.基于密码学的源认证机制主要可以分为两类:自认证(self-certifying)的地址以及基于证书的公钥密码机制.

自认证的地址是指网络实体在不依赖于第三方权威的情况下能够证明自己对所宣称地址的拥有权,从源头上解决地址欺骗的问题.自认证的思想最早由 Mazieres 等人提出[24],底层通常使用加密的方法.产生自认证地址最直接的方法是将地址与公钥绑定,使用对应的私钥对消息进行签名.接收方使用发送方的公钥对消息进行有效性认证,这样无需外部安全基础设施的支持就可以实现源地址真实性认证.由于公钥的长度往往大于命名空间的长度,在实际方案中通常使用公钥的 hash 值命名节点.目前,构造自认证地址的思想已经得到了广泛的采用,如:CGA[25]地址的低 64 位是由基于公钥等一系列参数的哈希散列产生;TrueIP[26]则将 IP 地址直接作为公共密钥;AIP[27]最核心的部分在于使用了 AD:EID 这种自我验证的地址形态,其中,AD 和 EID 分别是基于公钥散列产生的自治域及主机的全局唯一标识符.

基于证书的密码机制主要是针对源 AS 进行鉴别,即确认一个 BGP 发言者所在的 AS 是否具备宣告特定地址前缀的授权.其基本思想是:在 BGP 协议中增加 PKI(公钥基础设施,public key infrastructure)机制,通过提供 IP 前缀和自治系统号码的授权证明来主动防范非法的前缀宣告.从信任模型上又可以分为集中式和分布式两类:集中式认证方案[28−30]依赖于严格的层次式 PKI,以可信第三方为信任锚建立地址前缀、ASN(自治系统号)与公钥的绑定;而分布式认证[31,32]没有一致的信任根,需要选择出信任的对等实体.一般来说,集中式认证安全能力比分布式要强,但部署难度更大.

3.2 基于特征匹配的检测机制

该类机制借鉴了入侵检测的研究思路,通常包括两种基本组件:用于监测网络信息的监控设施以及提供匹配查询的网络特征库.基本思想是:将监测到的数据信息与事先采集的特征规则进行匹配,若发现异常行为,则进行报警或报文过滤.一般工作原理如图 4 所示.

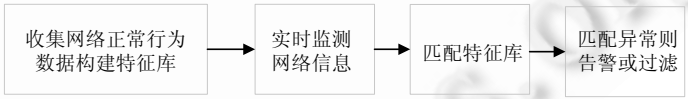


Fig.4 General working procedure of detective mechanisms

图 4 检测机制的一般工作过程

源地址欺骗的检测规则分为基于路由和基于报文标识两种类型:基于路由信息的检测是指路由器利用路由表中的地址前缀及接口链路等信息生成验证规则,判断分组的出入接口是否符合该规则,以此鉴别源地址欺骗报文.这些方案[33−37]大都需要全局部署,且存在一个普遍问题:无法处理同一接入子网内地址伪造的问题.基于报文标识是指在分组头部插入标记或对分组进行签名,在主机或者路径上的路由器中通过检测分组头部字段的方式进行非法报文的验证及过滤.这类方案[38−41]由于需要在报文中嵌入其他负荷,难免造成性能上较大的开销.另外,还有部分研究者专门针对源地址的定位提出了追踪回溯[42,43]方法,同样也是通过添加分组标记来加以实现,但由于事后处理的设计思想及复杂的回溯算法,使其没有得到广泛应用.

地址前缀劫持监测机制根据网络信息或流量特征的变化来判断是否有欺骗的发生,根据监测的数据类型,

可分为基于控制平面和数据平面两类:控制平面检测技术[44−46]大都采用被动监测路由信息(如路由更新报文)的方式,可部署性较好,但其检测结果的准确性和实时性都受到数据源的限制;基于数据平面的检测方法[47−49]多数要求设立若干观测点主动探测数据平面,根据观测到的特征(如传输路径或流量的变化)进行检测.另外,还有一些方案[50,51]尝试同时收集两个平面的信息进行综合分析,但其准确性同样受到来自两个平面数据源的共同约束.

3.3 基于地址空间分层的机制

IP 地址既充当定位符又作为标识带来了一系列路由可扩展性、移动性问题,为此,一些研究者们开始打破传统 TCP/IP 的限制,立足于创建 IP 地址身份和定位功能分离的体系结构[52−55].这些方案大都采用两层命名空间的思想,将地址空间分为身份标识和位置标识两部分,其中,身份标识用来标识主体身份,位置标识用来进行路由,两者之间由一个映射系统负责相互转换.这类机制按实现位置主要分为两类:一类在主机侧实现分离,如 HIP[56];另一类在边缘网络侧,由路由器等网络设备实现,如 LISP[57]等.图 5 以主机侧分离为例,说明了该机制的基本工作过程.

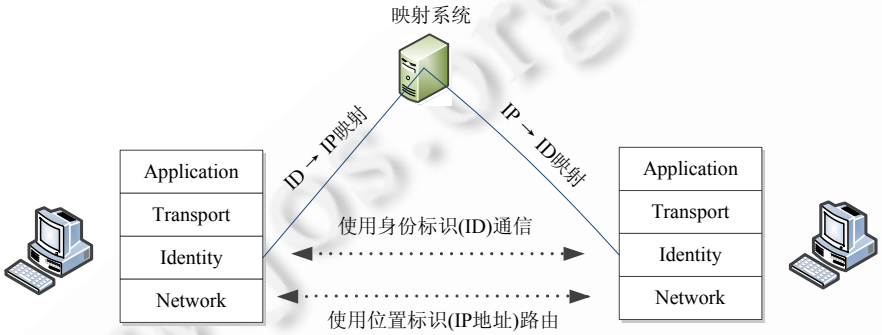


Fig.5 General principle of ID/LOC split mechanism

图 5 身份与位置分离机制的一般原理

尽管这类机制并没有将地址安全作为主要设计目标,但在其中一些方案(如 HIP)中,IP 地址只标识主机位置及用于路由,主机身份标识 HI(host identifier)基于主机公钥构造以保证其可信性.从地址生成技术来看,HIP 同样属于自认证的地址机制,但地址空间分层思想考虑了 IP 地址语义过载这一根本性问题,将身份与位置剥离开,对于将来地址结构的发展有着深刻的影响,因此,本文将 HIP 纳入这一机制中进行阐述.

3.4 地址安全机制分析

基于密码的源认证是一种欺骗避免机制,安全性好,但需要扩展地址和路由协议以及密码体系的支持,难免带来庞大的开销,实际部署难度大;攻击检测机制无法从根本上避免地址欺骗,只能进行事后的检测以降低攻击影响,但无需扩展协议,部署能力强,受到了研究者们的更多关注;地址空间分层机制从 IP 地址语义过载这一根本问题出发,旨在一体化地解决地址安全、路由可扩展以及移动性问题,但是部署迁移带来的开销也是相当可观的.地址安全机制的特点分析见表 1.

Table 1 Analysis of address security mechanisms

表 1 地址安全机制分析

地址安全机制	基本思想	安全手段	技术分类	代表方案	安全能力	可部署性
基于密码学的源认证	确认地址所有权	源绑定	自认证地址 PKI 证书	CGA[25] S-BGP[29]	强	较差
基于特征匹配的检测	构建信息特征库	异常特征匹配	控制平面 数据平面	PHAS[45] SAVI[37]	较弱	好
地址空间分层机制	身份位置属性分离	自认证地址	主机侧分离 网络侧分离	HIP[56] LISP[57]	一般	一般

4 互联网地址安全关键技术研究

在本节中,我们以实现地址安全的基本技术手段作为分类依据,结合一些典型方案简要加以阐述分析.

4.1 源地址安全关键技术

4.1.1 基于路由信息的分组过滤

基于路由信息是指路由器利用路由表中的地址前缀与接口链路的关系生成验证规则,通过检查流入的分组特征来验证是否为地址欺骗分组.

出入口过滤(ingress/egress filtering)[33]以 IP 前缀与子网的隶属关系作为验证规则,来判断是否为合法数据包.由边界网关路由器检查流入和流出的分组头部,对于一个边界网络内流出的数据包,若该数据包的源地址不属于该边界网络,则视其为欺骗数据包,称为出口过滤.同理,对于来自于该边界网络外部的数据包,如果这个数据包的源地址属于该边界网络,则判断其为源地址欺骗,称为入口过滤.该方案轻量且有效,但如果没有接近100%的部署率,则其效果将会大打折扣.

反向路径转发 RPF(reverse path forwarding)[34]在验证规则中引入了接口信息.RPF 认为:流入的任何源地址为 d 的分组,都将发送到目的地址为 d 的分组所转发的端口.也就是说,假如源地址为 d 的分组 P 从接口 1 进入,若路由表中没有⟨目的地址 d,接口 1⟩这一转发表项,则认为 P 是地址欺骗分组.但互联网中存在大量的不对称路由[58],势必造成一定的误判.

由于从特定源地址到特定目的地址所经过的链路是一定的,DPF(distributed packet filtering)[35]采用分布式过滤的方法.路由器通过维护路由信息来判断分组是否由错误的端口进入.假如一个攻击者想伪造一个源地址,他必须确保欺骗分组在每个经过的路由器中都由正确的端口进入.DPF 实现原理如图 6 所示:当节点 H 伪造节点 C 的报文时,节点 G 事先知道 C 的报文只会从固定的接口到达,因此丢弃 H 伪造的欺骗报文.实验结果表明,若有 18%的网络部署 DPF,就可以减少 90%的地址欺骗报文,但在 DPF 中并没有提供一种路由器获取报文到达链路的方法.近年来,一些基于 DPF 的域间源地址认证方案[59−61]都提出了相应的解决办法,比如在 IDPF(inter-domain packet filters)[59]中通过与直接邻居 AS 交换 BGP 消息来构建过滤规则,实现 IDPF 的路由器能够获取自治系统之间的关系信息,IDPF 根据这些策略来确定从发送方到接收方可能的上游 AS 集合,并以此作为在域间进行欺骗分组过滤的标准.

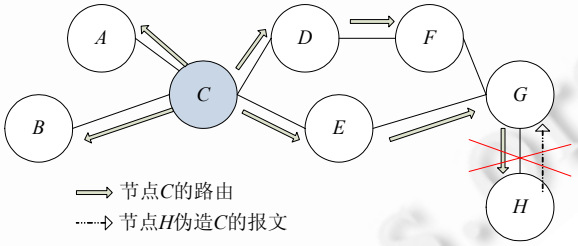


Fig.6 Detection in DPF

图 6 DPF 的检测原理

SAVE(source address validity enforcement protocol)[36]提供了一种路由信息更新的机制,以允许每个路由器建立一张与转发表相对应的进入表(incoming table).正如转发表关联了接口与特定的目的地址空间,进入表将每个接口与合法的源地址空间绑定在一起.当分组到达时,便可以通过进入表来判断分组是否合法.SAVE 在构建进入表时考虑了路由不对称带来的问题,但其更新消息的连续传递性,决定了无法进行增量式部署.

4.1.2 基于报文标识的地址认证

SPM(spoofing prevention method)[38]是一种域间地址验证方案,通过在报文中嵌入签名对来判断该数据包的合法性.源自治系统与目的自治系统共同协商一对动态变化的签名(s,d),其中,s 表示源自治系统,d 表示目的自治系统.当数据包发送时,源自治系统在报文中嵌入签名,到达自治系统 d 时,d 对数据包的签名进行检查.

SPM 开销较少,也具有较高的部署激励;但 SPM 是一种端到端的过滤机制,意味着路径中间的节点无法参与验证.

不同于 SPM 仅将目的自治域签名添加到报文中,Passport[40]添加所有经过的自治域签名.Passport 定义一个自身的头部,类似于一个具有多个“签证”的“护照”,每个签证对应着沿途经过的部署 Passport 的自治系统.当报文到达时,自治系统将验证护照里对应的签证信息(如图 7 所示).

Passport 中的“签证”其实就是一个消息认证码(message authentication code,简称 MAC),源自治系统使用与路径上每个 AS 共享的密钥计算出相应的 MAC,将其嵌入到发送的分组中.当下游路由器收到这个分组时,便可以利用与源自治系统共享的密钥重新计算 MAC 值,以此进行地址验证.与 SPM 相比,Passport 可以在伪造报文到达目的端之前进行过滤,但报文中嵌入的过多负荷造成了性能上的开销.

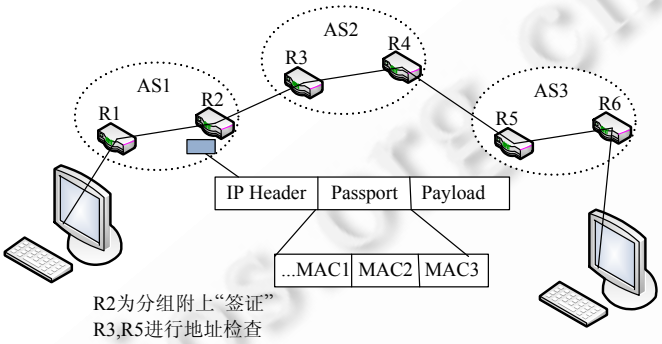


Fig.7 Illustration of passport

图 7 护照法示意图

StackPi[41]使用 TTL(time to live)作为分组标识域索引,并将标识域看作栈的形式.路径上支持 StackPi 的路由器分别将标记插入分组报文标识域.目的端接收到分组时并不清楚该分组的传输路径,但如果绝大多数分组都具有相同的标记,那么这些分组的传输路径则很可能是相同的.因此,一旦目的端系统识别出一个欺骗分组,即可过滤所有后续攻击报文.

HCF(hop-count filtering)[39]同样利用了分组的 TTL 变化规律,不同于 StackPi 的标记插入方式,HCF 通过构造一张精确的 IP 地址与跳数计数的映射表⟨IP-Count⟩来进行分组 TTL 的比对.

上述两种类型的部分方案已被路由器实际采用,在一定程度上减少了源 IP 地址欺骗的发生,但其关注面都比较单一,无法形成一套完整的地址认证安全体系.

2008 年,清华大学和 CERNET 网络中心提出了基于真实 IPv6 源地址的网络寻址体系结构 SAVA(source address validation architecture)[62],设计并实现了一种包括接入、域内、域间这 3 个层次的真实源地址验证系统,形成了一套有效而完整的源地址认证安全体系.接入子网的 IPv6 源地址验证目前的主要方案为 SAVI(source address validation improvements)[37],主要原理是将 IP 地址动态绑定到交换机的端口上,通过建立三元绑定关系⟨终端 IPv6 地址,终端 MAC 地址,接入设备的端口号⟩对流量进行过滤;自治域内源地址验证主要有入口过滤和 CPF 两种方案;域间使用的是 SMA(state-machine based anti-spoofing)[63],通过对 SPM 进行扩展,建立信任联盟以实现真实地址的验证.以清华大学(AS45576)、中国电信(AS4134)两个 AS 成员为代表,已经部署了 SMA 方案组成信任联盟(如图 8 所示),成员间彼此认证对方网络报文的真实性.

目前,SAVA 正逐步部署于我国最大的纯 IPv6 网络 CNGI-CERNET2 之中.另外,在 SAVA 的基础上,清华大学联合中国电信分别针对 IPv6 接入网环境以及 4over6 过渡场景中的源地址认证作了深入的研究,并向 IETF SAVI 工作组提交了两项标准草案[64,65].

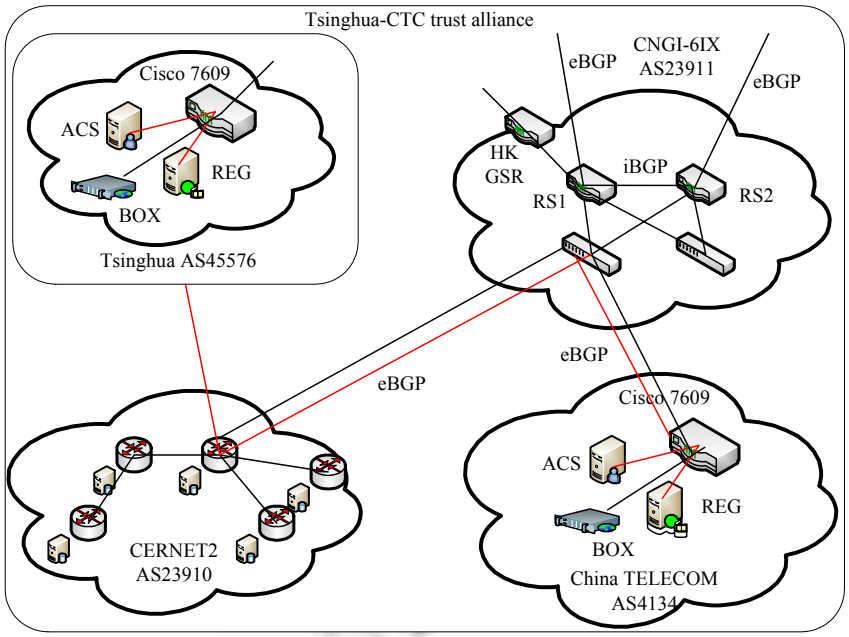


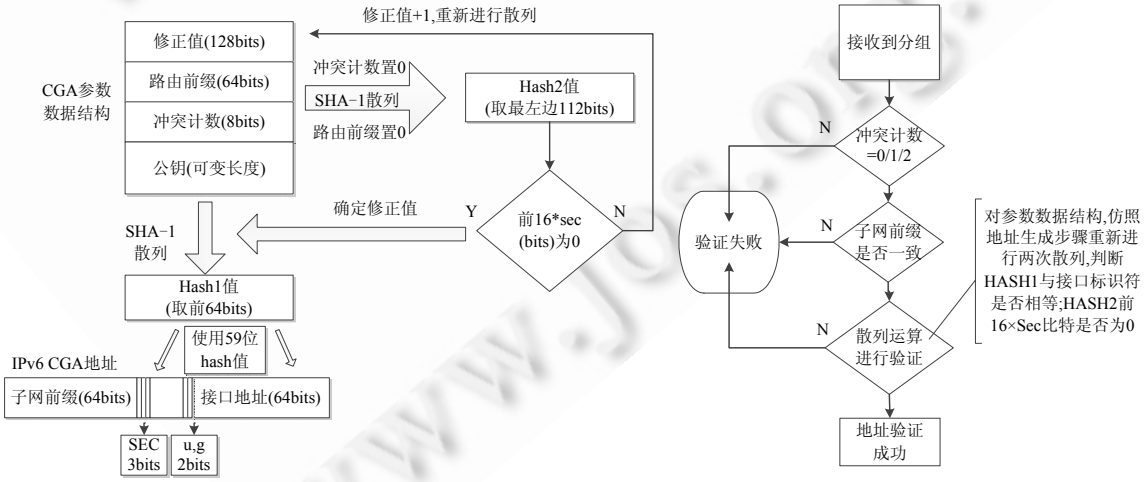
Fig.8 Illustration of trusted alliance of SAVA

图 8 SAVA 可信任联盟示意图

4.1.3 基于密钥构造的地址

利用加密产生地址的思想最初被应用于解决移动 IPv6 下的地址归属问题.为了保护 IPv6 网络中邻居发现协议(neighbor discovery protocol,简称 NDP)的安全性,IETF 的 SEND 工作小组提出了 CGA(cryptographically generated addresses,即加密产生的地址)的模型并标准化为 RFC[66].

CGA 基于公钥产生地址,地址结构类似于 IPv6,由 64 位子网前缀和 64 位接口标识符组成.不同的是,CGA 的接口标识符是利用地址所有者的公钥、安全参数 Sec 等辅助参数通过 hash 计算形成的.图 9(a)说明了 CGA 地址的结构及生成过程.



(a) CGA地址构造过程 (b) CGA地址验证过程

Fig.9 Data flows in generation and authentication of cryptographically generated addresses

图 9 CGA 地址构造与认证过程

发送方用相应的私钥对要发送的数据进行签名,并以CGA生成的地址连带CGA参数数据结构一起发送出去.CGA 接收方在收到数据后,通过对 CGA 参数重新散列等手段进行地址验证,具体验证步骤如图 9(b)所示.CGA的验证过程不需要额外的安全架构支持,但并不能确保经过认证的地址是否真的存在,且必须在部署了RSA 算法的网络环境中才能使用,网络管理的难度较大.

另一种基于密钥产生的地址是由 Schridde 等人提出的 TrueIP[26].TrueIP 的核心思想是通过 IBC(identity-based cryptography,简称 IBC)[67]构造地址.基于标识加密(IBC)的概念最早由 Shamir 提出,用以解决公共密钥的复杂管理问题.IBC 最大的优势在于使用了自认证的公共密钥.TrueIP 正是基于这一点,直接使用 IP 地址作为公钥,不需要 CA 或 PKI 将 IP 地址绑定到其他公钥上,有效地减小了管理开销.在 TrueIP 中,发送方利用私钥对数据进行签名,证明自己对某个 IP 地址的合法拥有权,接收方利用公钥对其进行验证.

4.1.4 源地址安全技术分析

针对源地址安全的技术方案种类较多,且涉及到路由协议及安全的多个领域.为了清晰、直观地进行分析比较,我们从以下几个维度对它们进行分类(见表 2):

1) 验证的粒度:能够验证何种粒度 IP 地址的真实性,网络前缀的验证或是细粒度网络接口地址的验证;
2) 验证的部署位置:地址安全机制的部署位置,可以是在源端的接入交换机、边界路由器或者目的端;
3) 验证规则生成手段:基于何种技术或信息生成验证规则,包括利用路由信息、在报文中嵌入标识等;
4) 过滤的位置:过滤欺骗分组的地点,在欺骗分组到达目的之前的路径上过滤或是到达端系统时过滤.

Table 2 Analysis of source address security technologies

表 2 源地址安全技术方案分析

验证方案	部署位置	过滤位置	验证规则生成	验证粒度
Ingress/Egress[33]	边界网络	路径上	路由信息	地址前缀
RPF[34]	边界网络	路径上	路由信息	地址前缀
DPF[35]	AS 间	路径上	路由信息	地址前缀
IDPF[59]	AS 间	路径上	路由信息	地址前缀
SAVE[36]	全网	路径上	路由信息	地址前缀
SPM[38]	AS 间	目的端	报文标识	地址前缀
Passport[40]	AS 间	路径上	报文标识	地址前缀
StackPi[41]	全网	目的端	报文标记	接口地址
HCF[39]	目的端	目的端	报文标记	接口地址
SAVA[62]	全网	路径上	多规则引擎	各层次粒度
CGA[66]	源主机	欺骗避免	自认证地址	接口地址

4.2 路由地址前缀安全关键技术

地址前缀劫持的根本原因在于前缀和前缀宣告方之间缺乏安全绑定,一种典型的技术是在路由协议中增加 PKI 机制来验证源 AS 的身份,确认其地址所有权;另一类是攻击检测技术,基本思想是前缀劫持发生后能够被及时探测从而进行报警和恢复.

4.2.1 基于密码的源 AS 认证技术

S-BGP(secure BGP)[29]是迄今为止相对完整的路由安全方案,采用两套 PKI,分别用于地址所有权以及 ASN(自治系统号)所有权认证,证书的签发并行于当前的地址分配系统,以 ICANN 为信任根,使用层次式的信任模型.ISP 拥有两类证书:IP 地址前缀证书和 ASN 证书,分别绑定了该地址前缀、ASN 与该 ISP 的归属关系.为了对源和路径进行认证,S-BGP 引入了一种可携带数字签名的路径属性,包括地址证明(address attestation,简称 AA)和路由证明(route attestation,简称 RA):

- AA 由地址前缀持有者产生,用来授予某 AS 宣告该地址前缀的权利;
- RA 被路径上的每个 AS 使用私钥依次签名,这种嵌套签名的方式,使 S-BGP 具备了较好的路径验证能力.

S-BGP 的具体验证方式如图 10 所示.

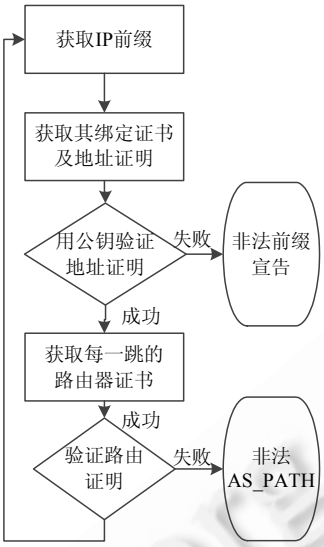


Fig.10 Authentication procedure of S-BGP

图 10 S-BGP 验证过程

soBGP(secure origin BGP)[30]是思科公司提出的一个轻量级方案,使用 3 类证书进行认证:EntityCert 通过将 AS 号与公钥绑定以进行身份认证;AuthCert 授权源 AS 宣告特定地址前缀;ASPolicyCert 包含与当前 AS 相邻的所有 AS 列表,BGP 路由器可以根据该证书计算出 AS 连接拓扑.BGP 发言人在收到路由信息时,便可根据此拓扑验证路径的真实性.soBGP 的源认证基于网状信任模型(Web of trust),无需严格的层次信任结构,但同时也相应降低了安全性;TBGP[71]定义了一组符合路由策略规范的更新与撤销规则,通过强制 BGP 路由器执行,从而形成一种信任传递关系,避免了仅仅依赖密码机制而带来的巨大开销.

S-BGP 具有强大的路由安全能力,但同时也存在开销大、部署难等实际问题.为此,研究者们在 S-BGP 的基础上展开了大量研究工作,关注重点在于如何减小密码机制带来的开销[68−70].

4.2.2 前缀劫持检测技术

基于控制平面的前缀劫持检测技术通常是将实时信息与历史数据的匹配结果作为检测规则,典型方案有 MyASN[44],PHAS(prefix hijack alert system)[45]和 Co-Monitor[46]等.

在 MyASN 中,用户首先需要注册,提供其所关注的地址前缀与源 AS 的映射关系;之后,MyASN 系统会将实时监测的映射关系与事先采集的映射信息相匹配,若发现已注册的前缀被非法宣告,则生成地址源变更事件.PHAS 类似 MyASN,区别在于其本身并不采集 BGP 路由信息,而是利用诸如 Route Views 等公共路由数据.Co-Monitor 基于“协作监测”的思想,让每个 AS 与其他参与者交换自定义的前缀-源自治系统映射信息,以形成一张全局映射表,同时监测本地 BGP 路由更新,一旦出现异常,则发出警报.

基于数据平面的检测技术主动发送探测数据包,并对返回的结果加以整理分析,从而进行检测判断.

一般来说,网络上某点到目标前缀的路径是稳定的,当该路径出现明显变化时,则怀疑发生前缀劫持.基于这种思想,Zheng 等人提出了一种分布式的检测方案[49].该方案周期性地探测从观测点到目标前缀的路径距离,并以是否发生显著变化为标准进行检测(如图 11 所示).ISPY[47]是一种用来检测自身前缀是否被劫持的方案,其基本思想是:如果 AS 遭到前缀劫持攻击,该 AS 发送的数据包将无法收到回应(即自治域不可到达),因为响应分组的目的地址已被劫持.同时,前缀劫持造成的污染会导致基于该 AS 的可达性视图出现很多“断路”.为了提高判断的准确性,ISPY 提出了“cut”值(即“断路”的数目)的概念,以区分自治域不可到达是否由前缀劫持所致.当“cut”值大于门限值时,则可判断前缀已被劫持.实验结果表明:门限值越大,误判的概率越小.类似的检测技术还有很多,如利用流量分布变化作为检测依据等[48],这里不再赘述.

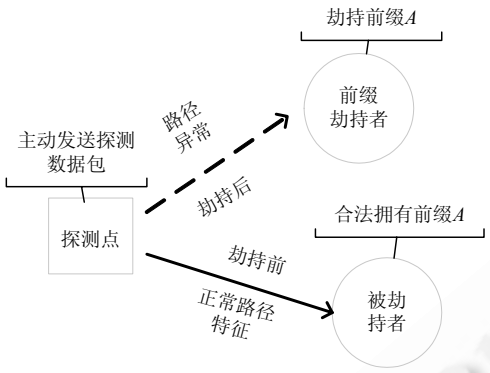


Fig.11 Detection based on path characteristic

图 11 基于路径特征的检测原理

综上可知:控制平面检测方法只需被动收集路由信息,实时性好,但检测结果的准确性在很大程度上受到数据集的限制;数据平面检测具备更强的部署能力,但需要不断地发送探测包,性能相对较低.

4.2.3 地址前缀安全技术分析

在 BGP 中,宣告非法地址前缀以及伪造 AS_PATH 都能够导致前缀劫持的发生[72],一种理想的前缀安全方案应当同时具备针对源以及路径的认证能力.基于密码的源认证技术通常具备路径认证能力,但计算和存储开销巨大;劫持检测技术可部署性好,但通常是以牺牲安全能力为代价.地址前缀安全技术分析见表 3.

Table 3 Analysis of routing address prefix security technologies

表 3 路由地址前缀安全技术分析

安全方案	验证方法	数据来源	源认证	路径认证	可部署性
S-BGP[29]	集中式信任模型	PKI 证书	强	强	较差
SoBGP[30]	网状信任模型	PKI 证书	强	弱	较差
MyASN[44]	源与前缀映射信息	控制平面	弱	–	较好
PHAS[45]	外部路由数据集	控制平面	弱	–	好
Distributed[49]	路径稳定性	数据平面	较弱	–	好
ISPY[47]	自治域可达性	数据平面	较弱	–	好

4.3 新型安全路由体系结构

如本文所述,地址安全方案数量众多,但通常关注面较为狭窄,而且大量的修补势必造成互联网的“臃肿不堪”.鉴于此,一些研究者提出了新型的安全路由寻址体系结构,旨在从根本上一体化地解决地址安全问题.

4.3.1 身份与位置分离的体系架构

主机标识协议 HIP(host identity protocol)[56]是一种典型的名址分离方案,最初由 Moskowitz 等人为解决 IP 网络中移动和多宿问题而提出.HIP 在传输层和网络层之间插入了一个独立的新协议层——主机标志层 HIL(图 12 展示了现有体系结构与 HIP 的对比),利用加密的命名空间为每个通信主机赋予一个全局唯一的主机标志 HI(host identity),而 IP 地址只用于数据包的路由与转发.

主机标识符 HI 使用公钥表示,每一个 HI 可映射到一个或多个 IP 地址,这些 IP 地址标记了移动节点在网络中的位置.由于非对称密钥算法中的公钥长度并不一致,因此,HIP 协议对 HI 进行单向散列变换,得到一个 128 位的主机标识标签 HIT(host identity tag),用于绑定 TCP 连接.主机标志层 HIL 负责传输层与网络层报文中 HIT 与 IP 地址的转换.这样就可以实现〈Identity,HIT〉以及〈Locator,IP〉的绑定,从而实现了传输层和网络层的分离.HIP 中,公钥的认证过程也就是主机身份的认证过程:在分组传递过程中,HIP 使用自己的私钥对分组数据进行签名,对等实体收到签名的数据后,再用发送端的公钥进行认证,从而保证数据源身份的真实可信.HIT 长度为 128bit,与 IPv6 的兼容性较好,但主机及应用的部署迁移将会是复杂而又庞大的工程,需要进一步的实践证明其

可用性.

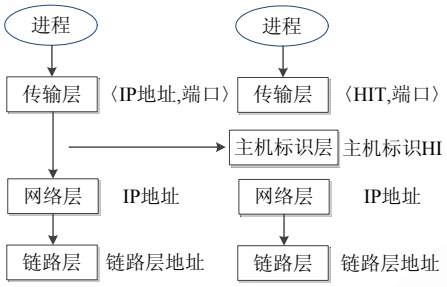


Fig.12 Layer structure of HIP

图 12 HIP 分层结构

4.3.2 基于责任性的安全路由体系

所谓责任性(accountability)是指将可靠的网络实体与网络行为绑定在一起的能力.近年来,accountability 的机制受到了业界的很大关注,并广泛用于解决网络体系结构中的安全问题.AIP[27]使用一种层次化的地址结构,使得网络层具有 accountability 的特性,并建立了一套完整的体系结构.AIP 的核心在于自认证的地址标识,它将每个网络单元划分成一个或者多个责任单元 Ads(accountability domains),每个 AD 都拥有全球唯一的 ID 号,为网络所在域(domain)的公钥 Hash 值;而 AD 中的每个主机唯一的终端号 EID,则是相应主机公钥的 Hash 值(其中,AD,EID 均为 160 位).因此在 AIP 体系结构中,主机就被表示为 AD:EID 的形式.

AIP 通过扩展逆向路径转发(uRPF)[73]来进行地址认证:在第 1 跳路由器处,通过签名回询的方式验证直接相连的主机地址是否真实;在分组穿越的每个 AD 中,使用 uRPF 验证上一跳路由器地址的真实性.具体验证过程如图 13 所示.

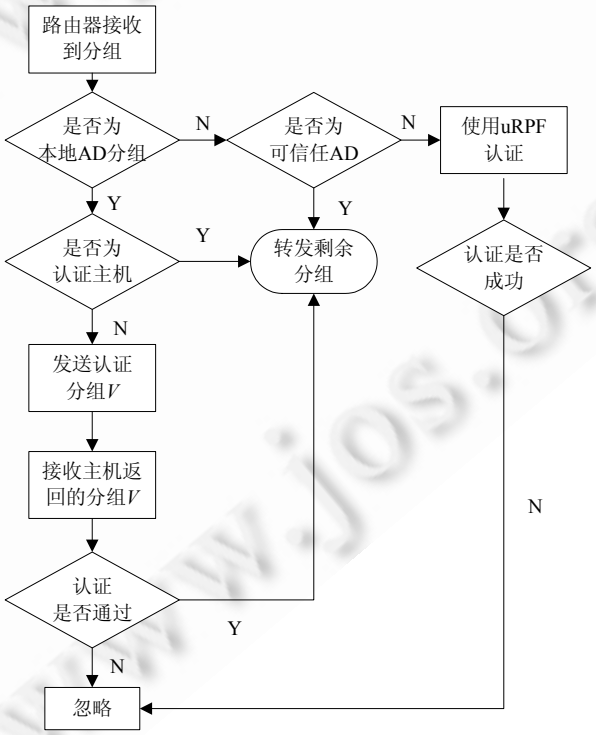


Fig.13 Process of address authentication in AIP

图 13 AIP 的地址验证过程

EID 地址的验证过程如下:假设第 1 跳路由器 R 接收到没有认证的主机发来的分组,那么它将丢弃该分组并返回一个认证分组 V,V 中包含源分组中的源和目的地址、分组的 hash 值以及分组到达接口这 3 种信息的编码形式.R 使用周期性更新密钥的 HMAC(Hash-based message authentication code)对 V 进行签名.源主机必须通过使用与其 EID 相关联的密钥对 V 进行签名来证明自身的真实性.如果主机产生了正确的签名,R 将缓存这条信息并正常转发剩余分组.AD 层对于非信任 AD 中的主机发送的分组则使用逆向路径转发(uRPF)进行验证,但是,由于 uRPF 在多宿主及路由不对称情况下存在缺陷,因此,AIP 通过结合发送认证分组的方式认证数据包的上一跳路由器的身份的真实性.

5 地址安全方案性能分析与评估

5.1 设计目标与难点

上一节分析了当前较为典型的地址安全方案的工作原理及特性.我们认识到,设计一种高效且易于部署的方案需要考虑到多方面的因素.一般来说,一种理想的地址安全技术方案应尽可能优化以下特性:

1) 地址欺骗防御能力:鉴别伪造地址(前缀)的能力,包括准确性、实时性等,还应结合追溯定位技术为审计追查提供基础;
2) 可部署性:对当前网络基础设施具备良好的兼容性,支持增量部署,为运营商提供部署激励;
3) 开销:方案的存储开销、计算开销、带宽开销等以及对网络性能造成的影响.

就目前来看,很少有哪一种方案或技术能够在各个方面都做得很优秀,安全能力与部署能力的矛盾始终是一个巨大的挑战.下面我们将当前典型的地址安全机制综合起来进行分析与比较.

5.2 地址欺骗防御性能

所有的地址安全方案根据自身的部署情况,都具备一定程度的防范能力.一般来说,使用密码体系的方案[29,30,40]安全能力更强;基于规则匹配的过滤机制[33−36]的安全性依赖于部署程度;就实时性而言,路径上的检测方案[40]在地址欺骗造成影响前阻断,比目的端检测[38]实时性要好;控制平面的前缀劫持检测[44−46]的实时性要优于数据平面[47−49];在追溯定位方面,由于 IP 追踪需要路由器添加相应标签以重组信息,所以端系统过滤的机制[38,39]大都不具备溯源能力;基于自认证地址的方案[26,56]以欺骗避免为目的,因此并没有考虑追溯定位.

5.3 可部署性

IP 分组头部部分字段的使用尚未标准化,基于对报文添加标识的方法[38−40]在实际部署时可能会产生一些不可预知的问题,因此可部署性不强.对于运营商的部署激励而言,过滤目的端欺骗分组的方案[38]比过滤源端[33]的要强.一部分自认证地址方案 CGA,TrueIP,HIP,AIP 沿用了类似 IPv6 的地址结构形式,也考虑到了与现有协议的兼容性,因此具备增量部署的特性,但部署迁移过程复杂.依赖全局 PKI 支撑的集中式源认证机制实际部署难度很大,若只在局部部署,安全性能则大打折扣.

5.4 开 销

地址安全的实现需以存储开销、计算开销及带宽开销为代价,这些开销也是部分地址安全机制至今不能实际部署的主要原因.基于 PKI 安全机制的方案[29,30]开销最大,自认证的地址基于密钥构造,同样有一部分计算和带宽开销.由于互联网“核心简单、边缘复杂”的设计思想,基于主机安全方案[40]的部署开销比基于路由器的要高.Ingress/Egress,RPF,DPF 在源端过滤 IP 欺骗报文,开销相对较小;SPM 及 Passport 需要维护一系列的签名信息,且存在路由器对流出分组进行标记并检查流入分组的计算开销;HIP 的实现需要在传统 TCP/IP 的传输层网络层之间添加新的协议层,且加密解密过程较为复杂.AIP 对现有网络体系结构进行了层次划分,增加了路由表数量,存储开销是需要解决的问题.

综合上述分析,我们在表 4 中对一些代表性方案的性能指标进行了总结.

Table 4 Analysis and evaluation on Internet address security mechanisms

表 4 互联网地址安全方案分析与评估

方案	安全目标	关键技术	验证粒度	防御能力	可部署性	开销
Ingress[33]	源地址安全	前缀与子网关系绑定	地址前缀	一般	较好	较小
DPF[35]	源地址安全	分布式接口信息维护	地址前缀	较好	较差	一般
SAVE[36]	源地址安全	前缀与接口关系绑定	地址前缀	较好	一般	一般
Passport[40]	源地址安全	路径上 AS 对分组签名	地址前缀	较好	较差	大
SAVA[62]	源地址安全	接口绑定、SMA 等	多粒度验证	好	较好	一般
CGA[66]	源地址安全	公钥构造自认证地址	接口地址	好	一般	较大
HIP[56]	源地址安全	地址分层及自认证地址	接口地址	好	较差	大
S-BGP[29]	路由前缀安全	基于 PKI 集中式认证	源、路径	好	差	大
SoBGP[30]	路由前缀安全	基于 PKI 网状信任模型	源、路径	较好	一般	较大
MyASN[44]	路由前缀安全	源 AS 与前缀映射信息	源 AS	较弱	较好	较小
PHAS[45]	路由前缀安全	外部路由数据集匹配	源 AS	较弱	好	小
Distributed[49]	路由前缀安全	路径距离特征变化	源 AS	一般	好	一般
ISPY[47]	路由前缀安全	AS 可达性视图变化	源 AS	较好	好	一般
AIP[27]	安全路由体系	自认证的层次化地址标识	各层次粒度	好	差	大

6 地址和标识通用实验管理平台

在众多地址安全解决方案中,安全性能与可部署性的矛盾是一个巨大的挑战,很难预测哪种方案未来将应用于互联网,目前也只有 S-BGP 进行过实际的部署实验.本文最后不是要提出一种地址安全方案,而是给出一种可以同时支持多种体系结构部署测试的通用实验平台的设想.在该平台中,可以对这些方案的实际性能和开销进行实验评估,并能给出一个直观的实验结果,从而进一步指出哪些特性会更加有利于实际部署.在这里,我们简单介绍一下通用实验平台的设计构想.

6.1 实验网络设计思想

从互联网体系结构的层次及基本组成来看,我们认为该实验平台可在地址、路由、传输这 3 个通用模型的基础上来进行设计,图 14 说明了实验网络平台的基本设计思路.

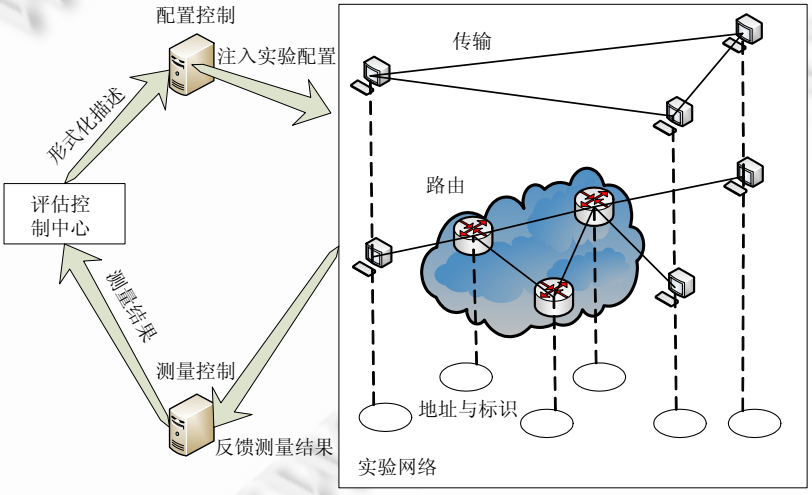


Fig.14 Basic structure of general experimental platform

图 14 通用实验平台的基本结构

首先,研究人员根据脚本描述规则,将实验方案抽象并形式化;评估控制中心通过配置控制服务器将实验配置部署到整个实验网络;测量控制服务器负责收集网络测量和实验结果,进行汇总向控制中心报告;控制中心针对不同性能指标,利用相应的评估方法[74]对被实验方案的可部署性、开销等特性进行量化评估.

6.2 地址和标识通用实验管理平台

在这一节中,我们将重点以通用的地址与标识部署平台为例,简要介绍一下其设计方法.

通用地址平台可以为不同的地址标识方案提供统一的部署实验环境.为保证最大程度的通用性和可伸缩性,我们首先需要提供一套语义完备的、可解释当前乃至未来地址属性的描述规范,研究人员基于这套规范就可以自定义出所需地址方案.比如说,我们可以对当前各种地址方案总结归纳,抽取出可以涵盖地址属性的核心特征,如地址类型、地址长度、前缀、构造方式、安全性、映射及资源需求等,研究人员只需给出这些特征的属性值,通用平台便可根据此描述将实际方案部署到实验网络中.例如,可对 IPv6 地址结构使用 XMLschema 定义描述规范(如图 15 所示).

```
〈?xml version="1.0" encoding="UTF-8"?〉
〈xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"〉
    〈xs:simpleType name="IPv6_Address"〉
        〈xs:restriction base="xs:string"〉
            〈xs:pattern value="([A-Fa-f0-9]{1,4}:){7}[A-Fa-f0-9]{1,4}"/〉
        〈/xs:restriction〉
    〈/xs:simpleType〉
    〈xs:element name="address_structure" type="hierarchical"/〉〈!--地址结构--〉
    〈xs:element name="address_blocks" type="xs:integer" fixed="8"/〉〈!--地址块--〉
    〈xs:element name="address_prefix" type="xs:integer"/〉〈!--网络前缀--〉
    〈xs:element name="separator" type="xs:string" fixed=":"/〉〈!--分隔符--〉
    〈xs:element name="base_address" type="xs:hexBianry"/〉〈!--地址基类型--〉
〈/xs:schema〉
```

Fig.15 Description of IPv6 address using XML

图 15 基于 XML 语言的 IPv6 地址描述

另外,我们还需要抽象出地址相关操作的通用原语和 API,使研究人员得以主动、可伸缩地参与和定制自己需要的地址与标识模型.例如:要在 IPv6 中增加 SAVI 机制,研究人员只需在上述描述规范中插入类似〈xs:sProperty="SAVI"/〉的描述,该平台将能自动调用对应 API 以及分配所需资源;在部署实验过程中,研究人员还可以通过定义完备的 API 控制 SAVI 的绑定信息、过滤策略等,以便让系统能够按照自己所期望的方式工作.这样,我们便可以通过控制安全机制的运作过程对该方案的性能和开销进行具体的实验评估.

7 总结和进一步的研究工作

当前,互联网体系结构不具备地址真实性验证机制,源地址伪造与路由地址前缀欺骗给互联网乃至社会稳定带来了极大危害.本文从研究体系、实现机制以及关键技术这 3 个维度对地址安全研究进行了归纳分析,并对典型地址安全方案的性能指标进行了总结评估.基于自认证地址以及身份与位置分离的思想,是当前乃至未来一段时间的研究热点.

尽管当前网络中已经部署了一些安全机制,但由于开销及兼容性等问题无法形成统一的安全体系,对于防范地址欺骗的效用是有限的.鉴于地址安全的重要性以及部署难题,从设计、部署、实验这 3 个角度来看,我们认为,未来的相关研究应包括以下 3 个方面:

(1) 解决安全性能与开销之间的矛盾.

本文中提到的基于密码的机制[25−30]虽然安全能力强,但大都使用了复杂加密算法以及需要全局 PKI 的支持,难以带来部署激励.目前,较新的研究都是在围绕如何减少加密开销的层面上[68−70].另外,在保证低开销的前提下,提高检测机制的准确性和实时性也是研究热点之一[47].

(2) 安全机制实际部署的策略与分析.

在现有的互联网体系结构中部署一种新机制,必须考虑到兼容性、开销等多方面的因素,而一种有效的部署策略也是值得深入研究的问题.如 Gill 等人[75]使用基于效用的模型对 S-BGP 的部署策略进行了分析,验证了

通过少数部署推动全网部署这一原则的有效性,对 S-BGP 的实际部署有一定的指导意义.

(3) 对地址安全方案进行针对性实验评估,从而得到其实际性能与开销的具体结论.

针对性的实验评估,有助于更加清晰地了解方案的具体性能参数,对方案的设计、研究以及部署具有重要的参考价值.从目前来看,GENI[76]是最为强大的实验平台,但系统庞大、复杂并缺少针对性指导原则,导致设计过于自由和发散.本文最后提出的通用地址与标识平台提供了对地址方案进行针对性实验及评估的可能.

致谢 感谢审稿专家对论文初稿提出的宝贵意见.

References:

[1] NewArch Project. Future—Generation Internet architecture. 2003. http://www.isi.edu/newarch/

[2] Postel J. Internet protocol—DARPA Internet program protocol specification. RFC 791, 1981. http://tools.ietf.org/html/rfc791

[3] Chun W, Lee TH, Choi T. YANAIL: Yet another definition on names, addresses, identifiers, and locators. In: Proc. of the CFI 2011. Seoul: ACM Press, 2011. 8−12. [doi: 10.1145/2002396.2002399]

[4] Wang JH, Wang Y, Xu MW, Yang JH. Separating identifier from locator with extended DNS. In: Proc. of the ICC 2012. IEEE, 2012. 2747−2751. [doi: 10.1109/ICC.2012.6363725]

[5] Steiner P. On the Internet, nobody knows you're a dog. 2013. http://en.wikipedia.org/wiki/Internet_Dog

[6] Manoj R, Tripti C. An effective approach to detect DDOS attack. In: Meghanathan N, ed. Advances in Computing and Information Technology. Berlin, Heidelberg: Springer-Verlag, 2013. 339−345. [doi: 10.1007/978-3-642-31600-5_33]

[7] Gilad Y, Herzberg A. LOT: A defense against IP spoofing and flooding attacks. ACM Trans. on Information and System Security (TISSEC), 2012,15(2):1−30. [doi:10.1145/2240276.2240277]

[8] Kumar S. Smurf-Based distributed denial of service (DDoS) attack amplification in Internet. In: Proc. of the ICIMP 2007. Washington: IEEE Computer Society, 2007. 25−35. [doi: 10.1109/ICIMP.2007.42]

[9] Li S, Zhuge JW, Li X. Study on BGP security. Ruan Jian Xue Bao/Journal of Software, 2013,24(1):121−138 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4346.htm [doi: 10.3724/SP.J.1001.2013.04346]

[10] Hiran R, Carlsson N, Gill P. Characterizing large-scale routing anomalies: A case study of the china telecom incident. In: Roughan M, Chang R, eds. Proc. of the Passive and Active Measurement. Berlin, Heidelberg: Springer-Verlag, 2013. 229−238. [doi: 10.1007/978-3-642-36516-4_23]

[11] Bangera P, Gorinsky S. Impact of prefix hijacking on payments of providers. In: Proc. of the 2011 3rd Int'l Conf. on Communication Systems and Networks (COMSNETS). IEEE, 2011. 1−10. [doi: 10.1109/COMSNETS.2011.5716486]

[12] MIT ANA spoofer project. 2013. http://spoofer.csail.mit.edu/

[13] Spoofer project: State of IP spoofing. 2013. http://spoofer.cmand.org/summary.php

[14] Beverly R, Berger A, Hyun Y. Understanding the efficacy of deployed internet source address validation filtering. In: Proc. of the ACM SIGCOMM 2009. Chicago: ACM Press, 2009. 356−369. [doi: 10.1145/1644893.1644936]

[15] YouTube hijacking: A RIPE NCC RIS case study. 2008. http://www.ripe.net/news/study-youtube-hijacking.html

[16] Kováčik M, Kajan M, Žádník M. Detecting IP spoofing by modelling history of IP address entry points. In: Doyen G, ed. Proc. of the Emerging Management Mechanisms for the Future Internet. Berlin, Heidelberg: Springer-Verlag, 2013. 73−83. [doi: 10.1007/978-3-642-38998-6_9]

[17] Wu JP, Wu Q, Xu K. Research and exploration of next-generation Internet architecture. Chinese Journal of Computers, 2008,31(9):1536−1548 (in Chinese with English abstract).

[18] Bellovin SM. A look back at "Security problems in the TCP/IP protocol suite". In: Proc. of the ACSAC 2004. Washington: ACM Press, 2004. 229−249. [doi: 10.1109/CSAC.2004.3]

[19] Dovrolis C, Streelman JT. Evolvable network architectures: What can we learn from biology? ACM SIGCOMM Computer Communication Review, 2010,40(2):72−77. [doi: 10.1145/1764873.1764886]

[20] Biersack E, Jacquemart Q, Fischer F, Fuchs J, Thonnard O, Theodoridis G, Tzovaras D, Vervier P-A. Visual analytics for BGP monitoring and prefix hijacking identification. IEEE Trans. on Network, 2012,26(6):33−39. [doi: 10.1109/MNET.2012.6375891]

[21] Feldmann A. Internet clean-slate design: What and why? ACM SIGCOMM Computer Communication Review, 2007,37(3):59−64. [doi: 10.1145/1273445.1273453]

[22] Kafle VP, Inoue M. Introducing multi-ID and multi-locator into network architecture. IEEE Trans. on Communications Magazine, 2012,50(3):104−110. [doi: 10.1109/MCOM.2012.6163588]

[23] Burness L, Eardley P, Jiang S, Xu XH. A pragmatic comparison of locator ID split solutions for routing system scalability. In: Proc. of the 3rd Int'l Conf. on ChinaCom 2008. 2008. 1024−1028. [doi: 10.1109/CHINACOM.2008.4685199]

[24] Mazières D, Kaminsky M, Kaashoek MF, Witchel E. Separating key management from file system security. In: Proc. of the 17th ACM SOSP. Charleston: ACM Press, 1999. 124−139. [doi: 10.1145/319344.319160]

[25] Rafiee H, Loewis MV, Meinel C. Transaction SIGnature (TSIG) using CGA algorithm in IPv6. Internet draft, 2013.

[26] Schridde C, Smith M, Freisleben B. TrueIP: Prevention of IP spoofing attacks using identity-based cryptography. In: Proc. of the SIN 2009. New York: ACM Press, 2009. 128−137. [doi: 10.1145/1626195.1626229]

[27] Andersen DG, Balakrishnan H, Feamster N, Koponen T, Moon D, Shenker S. Accountable Internet protocol (AIP). In: Proc. of the SIGCOMM 2008. New York: ACM Press, 2008. 339−350. [doi: 10.1145/1402946.1402997]

[28] Liu ZH, Sun B, Gu LZ, Yang YX. Origin authentication scheme against BGP address prefix hijacking. Ruan Jian Xue Bao/ Journal of Software, 2012,23(7):1908−1923 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4125.htm [doi: 10.3724/SP.J.1001.2012.04125]

[29] Kent S, Lynn C, Seo K. Secure border gateway protocol (S-BGP). IEEE Journal on Selected Areas in Communications, 2000,18(4):582−592. [doi: 10.1109/49.839934]

[30] White R. Securing BGP through secure origin BGP. Business Communications Review, 2003,33(5):47−53.

[31] Hu XJ, Zhu PD, Gong ZH. SE-BGP: An approach for BGP security. Ruan Jian Xue Bao/Journal of Software, 2008,19(1):167−176 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/19/167.htm [doi: 10.3724/SP.J.1001.2008.00167]

[32] van Oorschot PC, Wan T, Kranakis E. On interdomain routing security and pretty secure BGP (psBGP). ACM Trans. on Information and System Security (TISSEC), 2007,10(3):1094−9224. [doi: 10.1145/1266977.1266980]

[33] Baker F, Savola P. Ingress filtering for multihomed networks. RFC 3704, 2004.

[34] Wijnands IJ, Boers A, Rosen E. The reverse path forwarding (RPF) vector TLV. RFC 5496, 2009.

[35] Park K, Lee H. On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law internets. In: Proc. of the ACM SIGCOMM 2001. New York: ACM Press, 2001. 15−26. [doi: 10.1145/383059.383061]

[36] Li J, Mirkovic J, Wang MQ, Reiher P, Zhang LX. SAVE: Source address validity enforcement protocol. In: Proc. of the InfoCom 2002. New York: IEEE, 2002. 1557−1566. [doi: 10.1109/INFCOM.2002.1019407]

[37] Nordmark E, Bagnulo M. FCFS SAVI: First-Come, first-served source address validation improvement for locally assigned IPv6 addresses. RFC 6620, 2012.

[38] Bremler-Barr A, Levy H. Brief announcement: Spoofing prevention method. In: Proc. of the PODC 2004. Newfoundland: ACM Press, 2004. 375−375. [doi: 10.1145/1011767.1011832]

[39] Jin C, Wang HN, Shin KG. Hop-Count filtering: An effective defense against spoofed DDoS traffic. In: Proc. of the CCS 2003. New York: ACM Press, 2003. 30−41. [doi: 10.1145/948109.948116]

[40] Liu X, Li A, Yang XW, Wetherall D. Passport: Secure and adoptable source authentication. In: Proc. of the NSDI 2008. San Francisco: USENIX Association, 2008. 365−378. https://www.usenix.org/legacy/events/nsdi08/tech/full_papers/liu_xin/liu_xin.pdf

[41] Yaar A, Perrif A, Song D. StackPi: New packet marking and filtering mechanisms for DDoS and IP spoofing defense. IEEE Journal on Selected Areas in Communications, 2006,24(10):1853−1863. [doi: 10.1109/JSAC.2006.877138]

[42] Yang MH, Yang MC. RIHT: A novel hybrid IP traceback scheme. IEEE Trans. on Information Forensics and Security, 2012,7(2):789−797. [doi: 10.1109/TIFS.2011.2169960]

[43] Saurabh S, Sairam AS. Linear and remainder packet marking for fast IP traceback. In: Proc. of the COMSNETS 2012. Bangalore: IEEE, 2012. 1−8. [doi: 10.1109/COMSNETS.2012.6151318]

[44] RIPE. Routing information service: MyASn system. 2013. http://www.ripe.net/data-tools/stats/ris/routing-information-service

[45] Lad M, Massey D, Pei D, Wu YG, Zhang BC, Zhang LX. PHAS: A prefix hijack alert system. In: Proc. of the15th USENIX Security Symp. Vancouver: USENIX Press, 2006. 153−166. http://static.usenix.org/events/sec06/tech/lad.html

[46] Liu X, Zhu PD, Peng YX. Co-Monitor: Collaborative monitoring mechanism for detecting prefix hijacks. Ruan Jian Xue Bao/ Journal of Software, 2010,21(10):2854−2598 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3657.htm [doi: 10.3724/SP.J.1001.2010.03657]

[47] Zhang Z, Zhang Y, Hu YC, Mao ZM, Bush R. Ispy: Detecting ip prefix hijacking on my own. IEEE/ACM Trans. on Network, 2010,18(6): 1815−1828. [doi: 10.1109/TNET.2010.2066284]

[48] Liu YJ, Su JS, Chang RKC. LDC: Detecting BGP prefix hijacking by load distribution change. In: Proc. of the 2012 IEEE 26th Int'l Parallel and Distributed Processing Symp. Workshops & PhD Forum. IEEE, 2012. 1197−1203. [doi: 10.1109/IPDPSW.2012.147]

[49] Zheng CX, Ji LS, Pei D, Wang J, Francis P. A light-weight distributed scheme for detecting IP prefix hijacks in real-time. In: Proc. of the SIGCOMM 2007. Kyoto: ACM Press, 2007. 277−288. [doi: 10.1145/1282380.1282412]

[50] Xiang Y, Wang ZL, Yin X, Wu JP. Argus: An accurate and agile system to detecting ip prefix hijacking. In: Proc. of the ICNP 2011. Beijing: IEEE, 2011. 43−48. [doi: 10.1109/ICNP.2011.6089080]

[51] Hu X, Mao ZM. Accurate real-time identification of IP prefix hijacking. In: Proc. of the IEEE Symp. on Security and Privacy. Oakland: ACM Press, 2007. 3−17. [doi: 10.1109/SP.2007.7]

[52] Xu X. Routing architecture for the next generation Internet (RANGI). 2009. http://tools.ietf.org/id/draft-xu-rangi- 02.txt

[53] Shang WT, Bao CX, Li X. Research and comparison on the ID/locator separation network architecture. In: Proc. of the 2nd Int'l Conf. on CECNet 2012. IEEE, 2012. 1198−1203. [doi: 10.1109/CECNet.2012.6202059]

[54] Kafle VP, Li RD, Inoue D, Harai H. An integrated security scheme for ID/locator split architecture of future network. In: Proc. of the 2012 IEEE Int'l Conf. on Communications (ICC). IEEE, 2012. 5866−5871. [doi: 10.1109/ICC.2012.6364739]

[55] Kanemaru S, Yonemura K, Teraoka F. ZNP: A new generation network layer protocol based on ID/locator split considering practical operation. In: Proc. of the 2011 IEEE Int'l Conf. on Communications (ICC). 2011. 1−6. [doi: 10.1109/icc.2011.5963378]

[56] Moskowitz R, Hirschmann V, Jokela P, Henderson T. Host identity protocol version 2 (HIPv2). 2013. https://datatracker.ietf.org/doc/draft-ietf-hip-rfc5201-bis/

[57] Farinacci D, Fuller V. The locator/ID separation protocol (LISP). RFC 6830, 2012.

[58] Rodríguez A, Ruiz R. A study on the effect of the asymmetry on real capacitated vehicle routing problems. Computers & Operations Research, 2012,39(9):2142−2151. [doi: 10.1016/j.cor.2011.10.023]

[59] Duan ZH, Yuan X, Chandrashekar J. Constructing inter-domain packet filters to control IP spoofing based on BGP updates. In: Proc. of the InfoCom 2006. Barcelona: IEEE, 2006. 1−12. [doi: 10.1109/INFOCOM.2006.128]

[60] Velmayil G, Pannirselvam S. Defending of IP spoofing by ingress filter in extended-inter domain packet key marking system. Int'l Journal of Computer Network and Information Security (IJCNIS), 2013,5(5):47−54. [doi: 10.5815/ijcnis.2013.05.06]

[61] Abhang TA, Kulkarni UV. An integrated approach to detect and limit IP spoofing. Int'l Journal of Computer Science and Mobile Computing, 2013,7(2):59−65. http://www.ijcsmc.com/docs/papers/July2013/V2I7201326.pdf

[62] Wu J, Bi J, Li X, Xu K, Williams M. A source address validation architecture (SAVA) testbed and deployment experience. RFC 5210, 2008.

[63] Liu BY, Bi J. SMA: State machine based anti-spoofing. 2013. http://www.paper.edu.cn/en_releasepaper/content/4514654

[64] Xu K, Zhu L, Hu G. SAVI requirements and solutions for ISP IPv6 access network. 2012. https://datatracker.ietf.org/doc/draft-shi-savi-access/

[65] Xu K, Hu G, Bi J, Xu M. The requirements and tentative solutions for SAVI in IPv4/IPv6 transition. 2012. https://datatracker.ietf.org/doc/draft-shi-savi-access/

[66] Aura T. Cryptographically generated addresses (CGA). RFC 3972, 2005.

[67] Hoeper K, Gong G. Bootstrapping security in mobile ad hoc networks using identity-based schemes with key revocation. Technical Report, CACR 2006-04, Centre for Applied Cryptographic Research, University of Waterloo, Canada, 2006. 1−25. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.88.7797

[68] Mancini LV, Spognardi A, Soriente C, Villani A. Relieve Internet routing security of public key infrastructure. In: Proc. of the 21st Int'l Conf. on Computer (ICCCN). IEEE, 2012. 1−9. [doi: 10.1109/ICCCN.2012.6289235]

[69] Wählisch M, Maennel O, Schmidt TC. Towards detecting BGP route hijacking using the RPKI. ACM SIGCOMM Computer Communication Review, 2012,42(4):103−104. [doi: 10.1145/2377677.2377702]

[70] Raimagia D, Singh S. A trusted centralized public key to secure border gateway protocol. IJEIR, 2012,3(1):226−230.

[71] Li Q, Xu MW, Wu JP, Zhang XW, Lee PPC, Xu K. Enhancing the trust of internet routing with lightweight. In: Proc. of the ASIACCS 2011. Hong Kong: ACM Press, 2011. 92−101. [doi: 10.1145/1966913.1966927]

[72] Zhang Y, Pourzandi M. Studying impacts of prefix interception attack by exploring BGP AS-PATH prepending. In: Proc. of the 2012 IEEE 32nd Int'l Conf. on ICDCS. IEEE, 2012. 667−677. [doi: 10.1109/ICDCS.2012.59]

[73] Ferguson P, Senie D. Network ingress filtering. RFC 2827, 2000.

[74] Xu K, Zhu M, Lin C. Internet architeture evaluation models, mechanisms and methods. Chinese Journal of Computers, 2012,35(10): 1985−2006 (in Chinese with English abstract). [doi: 10.3724/SP.J.1016.2012.01985]

[75] Gill P, Schapira M, Goldberg S. Let the market drive deployment: A strategy for transitioning to BGP security. In: Proc. of the SIGCOMM 2011. Toronto, 2011. 14−25. [doi: 10.1145/2043164.2018439]

[76] GENI. http://www.geni.net

附中文参考文献:

[9] 黎松,诸葛建伟,李星.BGP 安全研究.软件学报,2013,24(1):121−138. http://www.jos.org.cn/1000-9825/4346.htm [doi: 10.3724/SP.J.1001.2013.04346]

[17] 吴建平,吴茜,徐恪.下一代互联网体系结构基础研究及探索.计算机学报,2008,31(9):1536−1548.

[28] 刘志辉,孙斌,谷利泽,杨义先.一种防范 BGP 地址前缀劫持的源认证方案.软件学报,2012,23(7):1908−1923. http://www.jos.org.cn/1000-9825/4125.htm [doi: 10.3724/SP.J.1001.2012.04125]

[31] 胡湘江,朱培栋,龚正虎.SE-BGP:一种 BGP 安全机制.软件学报,2008,19(1):167−176. http://www.jos.org.cn/1000-9825/19/167.htm [doi: 10.3724/SP.J.1001.2008.00167]

[46] 刘欣,朱培栋,彭宇行.Co-Monitor:检测前缀劫持的协作监测机制.软件学报,2010,21(10):2584−2598. http://www.jos.org.cn/1000-9825/3657.htm [doi: 10.3724/SP.J.1001.2010.03657]

[74] 徐恪,朱敏,林闯.互联网体系结构评估模型、机制及方法研究综述.计算机学报,2012,35(10):1985−2006. [doi: 10.3724/SP.J.1016.2012.01985]

徐恪(1974−),男,江苏洪泽人,博士,教授,博士生导师,CCF 高级会员,主要研究领域为新一代互联网体系结构,高性能路由器体系结构,P2P 与应用层网络,Overlay 网络,物联网.

E-mail: xuke@mail.tsinghua.edu.cn

朱亮(1982−),男,博士生,主要研究领域为计算机网络体系结构,网络安全.

E-mail: tshbruce@gmail.com

朱敏(1977−),女,博士生,主要研究领域为计算机网络体系结构及其评估.

E-mail: min-zhu09@mails.tsinghua.edu.cn