真实源地址验证

设计背景 P8

IP地址唯一标识互联网中每台设备，在通信中充当发件人和收件人地址。

伪造源IP地址是非常简单的，构造IP数据包头时可以随意填一个IP地址

网关在进行数据包转发时，**不会验证**数据包中源IP地址是否来自网关所在的局域网中

基于 IP 地址伪造的攻击 P11

不伪造特完地址

目的是隐藏自身信息，使得目的主机即使被攻击，也无法追溯到攻击源， 避免网络审查，不伪造特定地址不是不伪造地址。

攻击者随机伪造许多IP地址，同时向目的主机发送服务请求；目的主机的资源因为大量请求而占满，无法再响应其他请求，甚至直接崩溃。

伪造特定地址

基于特定IP地址和目的主机的信任关系， 伪造特定IP地址取得目标主机的信任以执行恶意指令或获取机密信息。

利用DDoS攻击使被攻击主机暂时停止响应目的主机

猜测出被攻击主机和目的主机之间连接标识信息， 达到与目的主机连通

向目的主机发送恶意脚本执行恶意指令，实现破坏目的主机，获取机密信息，甚至控制目的主机

危害严重 P13

IP协议是互联网的核心底层协议，源IP地址真实性的缺失影响到互联网体系结构的各个层面。基于IP的上层协议使用IP地址这个并不安全的标识作为通讯对方的标识，因而只要伪造了源地址，相应地就欺骗了这些协议，这使得伪造源地址攻击的能力超出网络层范围，危害到其它层的协议。

利用源地址伪造的手段，网络攻击的发起者可以隐匿自己的身份和位置，逃避法律的制裁。

基于真实地址的网络计费、管理、监控和安全认证等都无法正常进行，对互联网基础设施和上层应用都造成了严重的危害。

现有防御方法 P15

防御种类	方法	简介	缺点
数据包签名	SPM、Pasport，StackPi、Base等	在IP包头中的ToS或其它较少使用的选项字段加入用户身份鉴别标签	假冒者可以学习标签的添加方法，从而逃避验证
数据包签名	HIP	修改用户终端主机协议栈，在IP和传输层之间添加“主机标识层”	端系统的修改、应用存在着实际困难
出流量源地址检测	Ingress Filtering	路由器根据出流量源IP是否在该路由器所属网络内进行过滤	配置过于复杂
出流量源地址检测	uRPF	根据数据包的源地址反查路由表，判断转发端口是否与数据包的入端口一致	无法防止同方向上的地址假冒，同时路由的非对称性也可能导致假阳性的误判
出流量源地址检测	SAVE	通过为路由器提供拓扑、时钟等附加信息设计整套数据包验证及其路由机制	协议过于复杂并且需要修改用户主机协议栈

现有方法的缺陷 P16

现有源地址验证技术相互独立，只能部分地解决源地址验证的问题，没有形成一个完整的覆盖整个网络的整体结构

- 算法复杂，协议开销大
- 缺乏部署激励
- 完备性不足
- 可扩展性不足

真实 IP 原地址的三重含义 P19

真实IPv6源地址验证体系结构，用以在网络层提供一种透明的服务，确保互联网中转发的每一个分组都使用“真实IP源地址”

1. 经授权的：IP源地址必须是经互联网IP地址管理机构分配授权的，不能伪造
2. 唯一的：IP源地址必须是全局唯一的
3. 可追溯的：网络中转发的IP分组，可根据其IP源地址找到其所有者和位置

真实源地址验证体系结构 SAVA P20

SAVA体系结构的三层结构包括接入子网层、自治系统内部层和自治系统间层。

1. 接入子网层：该层位于 SAVA 体系结构的最底层，负责对直接接入网络的主机进行源地址验证。在这一层，SAVA 设备会绑定主机和其IP地址，并验证从主机发出的数据包是否使用了正确的源地址。这一层的作用是防止本地网络中的源地址伪造攻击，确保只有合法的主机才能发送具有正确源地址的数据包。
2. 自治系统内部层：该层位于 SAVA 体系结构的中间层，负责在自治系统内部进行源地址验证。在自治系统内

部的路由器上进行源地址验证，以确认数据包的源地址确实来自预期的接入点。这一层的作用是防止自治系统内部的源地址伪造，确保数据包的源地址符合预期的接入点。

3. 自治系统间层：该层位于 SAVA 体系结构的最顶层，负责在不同自治系统之间进行源地址验证。在自治系统间的路由器上进行源地址验证，以确认数据包的源地址确实来自预期的自治系统。这一层的作用是防止不同自治系统之间的源地址伪造，确保数据包的源地址符合预期的自治系统。

组织特点

不同层次实现不同粒度的IPv6源 地址真实性验证；每一层次，允许不同运营商采用 不同方法；整体结构简单性和各部分组成的 灵活性的平衡

部署收益

1. 安全责任明确：易于追踪攻击事件，定位攻击者；杜绝基于伪造源地址的攻击
2. 网络管理简化：简化身份认证；流量可审计不可抵赖；支持基于IP地址的网络计费

真实源地址验证体系结构设计原则

1. IPv4地址结构：P23~25
2. IPv6地址结构：P26~27
3. 自治域 P28
4. 域内路由 IGP-OSPF：P29~33
5. 域间路由 BGP：P34~37

SAVA设计原则：P38

可扩展性 P38~45

采用层次化的思想来满足体系结构可扩展性需求是一种常用的手段；各层之间可以共同协作，根据约定俗成的协议进行简单交互而不用关注对方内部的实现细节，大大提升体系的效率。

- 层与层之间相独立，每层可以独立进行技术的演化
- 每层拥有自己的优化目标
- 不同层次利用局部信息对决策进行分布式计算，以实现个体最优
- 综合起来，这些局部算法实现了全局最优

需要划分灵活可变的源地址验证粒度，满足不同部署区域的需求和整体架构的可扩展性需求。需要建立层次化，寻找合理的层次间关系，使得各层之间可以共同协作，同时避免层次之间的过度依赖。

可演进性 P46

1. 与已有协议兼容：SAVA体系结构建立在当前互联网体系结构基础上，整体的技术依附于现有体系结构实现，因此必须要求技术对应协议与现有体系结构协议兼容
2. 自身部署可演进：SAVA的部署是一个持续性的过程，所以会出现部分区域已经部署SAVA，而部分区域尚 未部署SAVA的情况，需要考虑在发展部署的过渡阶段SAVA自身的兼容性
3. 运营商之间可演进：考虑到网络中不同运营商的存在，SAVA体系结构还应允许运营商可以采用各自不同的实现，SAVA系统各部分相互独立，且功能彼此不依赖

安全性 P47

SAVA体系结构的构建是支撑真实可信互联网体系结构实现，通过将安全性赋予现有体系 结构，弥补其信任缺失的问题，所以保障SAVA自身的安全性至关重要

1. 可信标识风险：标识应当具备唯一性、可追溯性
2. 数据转发风险：需保证携带标签的数据包转发中不被篡改，即使篡改也应被及时并准确地识别
3. 单点信任风险：标签的验证应当不依赖于中心化的网络基础设施，以免引入网络基础设施的信任风险

SAVA体系结构与关键技术 P50

部署与地址管理范围的失配问题 P50

源地址在分配上存在层次性。自治域从区域的地址分配机构 RIR获取多个前缀，这些前缀在被 拆分为更细粒度的前缀之后被分配到自治域内的各个子网。主机在使用地址时，需要从所接入的子网获取地址。在早期SAVA的研究中，很自然地将源地址验证划分为自治域、前缀、主机这三个粒度。随着真实源地址验证技术的发展和应用的增量部署，出现一个自治域中部分子网部署了真实源地址验证技术，而剩余子网尚未部署的情形，这就导致SAVA部署与地址管理范围的失配。

面向地址域的新型源地址验证SAVA体系结构 P51~52

地址域：同一机构所属的全部IP地址中的可部分管理范围

- 以一个校园网为例，地址域可以是某一个院系下的某个所某个组，也可以是某个所、某个院系，甚至可以是整个校园网
- “地址域” 显著提升体系结构的灵活性，实现了部署结构灵活的源地址真实性验证体系结构
- 接入网、地址域内和地址域间三层结构，具有松耦合、多重防御、支持增量部署等优点

1. 接入层面提供主机粒度的源地址验证能力，以保证地址使用的可追溯性
2. 在地址域内层面提供前缀级别的保护能力，以保护核心设备不被攻击
3. 在地址域间层面提供地址域级别的联盟内可验证能力以及保护自身不被依造的能力

SAVI实现源地址验证的“三步曲” P54

1. 获取合法地址：监听控制类报文（如ND、DHCPv6），即CPS分组，获取地址分配信息以识别主机合法IP源地址
2. 建立绑定关系：将合法的IP地址与主机网络附属的链路层属性绑定（“绑定锚”）（可验证的，且比主机的IP源地址本身更难欺骗）
3. 匹配验证：对数据包中的IP源地址与其绑定锚进行匹配（**部署位置越靠近主机，有效性越高**）

接入网异构多样性 P55

1. 终端多样性：终端包括手机、电脑、服务器、嵌入式设备等各种类型设备，即使同一种设备， 其上运行的系统也可能不同，比如手机可能是安卓系统，也可能是IOS系统
2. IP分配方式多样性：包括DHCP协议分配、SLAAC协议分配、静态配置等
3. 接入方式多样性：包括有线、无线等，不同接入模式可用的邦定锚可以不同

SAVI 验证方式 P56

针对多种接入网技术、多种地址分配方式、多种终端类型，SAVI设计了各种对应的验证方式

- 所有相关网络设备在同一个网络管理机构管理控制下
- 解决方案与接入子网地址管理分配和控制策略密切相关
- 解决方案与端系统的接入方式密切相关

DHCP P57~59

1. 允许主机在加入网络时从网络服务器动态获取IP地址
2. 在使用中的地址可以更新租期
3. 允许地址重用(仅在连接on时保留地址)
4. 支持想要加入网络的移动用户

无线局域网 WLAN P60~61

WLAN网络架构分有线侧和无线侧两部分；有线侧是指接入点AP上行到Internet的网络使用以太网协议；无线侧使用802.11协议，连接终端STA和AP，又称WiFi；无线侧包括基于控制器AC的AP架构（瘦AP，FitAP）和传统的独立AP架构（胖AP，Fat AP）。

无线 SAVI P62

基于无线局域网的源地址认证技术通过嗅探地址分配相关控制报文（如NDP和DHCP报文），将IP地址与MAC地址绑定并依赖MAC地址的安全性对伪造IP源地址的报文进行过滤。增加对主机移动场景的支持，提升了SAVI的灵活性。

802.1x 认证 P63

802.1x是一种对用户进行认证的链路层协议。802.1x是基于端口的认证策略（可以是物理端口也可以是VLAN一样的逻辑端口，相对于无线局域网“端口”就是一条信道）。802.1x的认证的最终目的就是确定一个端口是否可用。802.1x认证通过后，将成为用户IP地址的绑定锚。

动态自适应的地址分配分组监听 P64~65

SAVI-DHCP等方法通常被视为彼此独立的，每个方法处理自己的条目。如果在同一设备中使用了多种方法而没有进行协调，每一种方法都会拒绝通过其他方式绑定的数据包；SAVI设计了SAVA-MIX统一管理绑定表，基于各种方式形成了动态自适应的地址分配分组监听。

一旦某种SAVI方法生成了IP地址和对应绑定锚，它将请求SAVI-MIX在绑定表中设置相应的条目。SAVI-MIX将检查绑定表中是否有任何冲突。如果没有冲突，将生成一个新的绑定条目。如果有冲突，将按照一定策略进行冲突解决。

对现有网络设备和主机协议栈透明（不修改协议、不修改主机），能够适应复杂、动态、大规模的实际网络环境。实现了地址级的无漏判源地址验证，并且通过将设备标识与合法IP地址关联，达到了端网协同的目标，同时也实现了接入网兼容性。

SAVI 技术方案概要 P66

主要步骤

1. 监听地址分配协议的控制报文，确定合法的IP源地址
2. 将合法的IP地址绑定到主机的链路层属性 (绑定锚)
3. 对数据包中的IP源地址与它们所绑定的绑定针是否匹配进行检验

实施效果

1. 附着在同一接入设备下的主机不能伪造本接入设备下 其余主机的IP地址
2. 附着在某一接入设备下的主机不能伪造其他接入设备 下主机的IP地址

域内真实源地址验证 P67

1. 如果一个地址域与接入网相连，需保证从接入网流入地址域的流量，其源地址不会假冒该接入网之外的地址
2. 如果接入网部署了SAVI，进行二次验证；如果接入网没有部署SAVI，缩小源地址假冒的范围（接入网级别）
3. 保证从地址域内产生并流出地址域的流量，其源地址不会假冒地址域之外的地址

精准过滤：地址过滤的精确率（precision）100%；地址过滤的召回率（recall）100%

自动更新：自适应接入网地址分配和域内路由策略的动态更新，不完全依赖手动配置

原地址验证表 SAVA-P P68

根据目的地址选择分组的出接口（**路由转发表**）

根据源地址验证分组的入接口（**源地址验证表**）

P70 源地址验证表生成方法

1. 正确性：解决路由不对称问题
2. **低开销**：通信开销和计算开销
3. **激励性**：网络通过主动部署受益

基本思路和基本框架 P71~73

路由器通过发送探测报文，探测域内转发咯径，沿途的路由器根据收到的探测报文生成<源前筑和入接口>的对应关系。

利用FIB中的destination prefix指导探测报文的接力发送方向；考虑到域内策略路由的复杂性，路由器无法获知到destination prefix的准确路径信息；一个探测报文携带去往同一个下一跳的多个destination prefix，减少传输开销。

DPP 报文的生成与处理 P74~85

P74 原始DPP报文的生成及其格式，P75~76 路由器收到DPP报文的处理方式，P81 路由器收到多个同源DPP的四种场景，P82 路由环路检测，P83 开销分析，P84 实验分析

方案总结 P85

牴计三妄	URPF [RFC 3704, 8704]	SAVE [INFOCOM 2002]	O-CPF [CFI 2013]	SAVA-P
正确性（解决路由不对称问题）		V	V	建立与转发表方向相反的源地址验证表，克服路由不对称问题
低开销（通信开销和计算开销）	V			每台路由器处理的协议报文数量约为O(N)，N为网络内的路由器数量

域间真实源地址验证 SAVA-X P86

通过在地址域之间建立信任联盟实现源地址验证，部署在联盟成员的边界路由器上；边界路由器为本域内发往其它联盟成员的报文进行地址域级别的源地址前缀检查，保证源自本地址域的报文携带的源地址确实属于本地址域；边界路由器为源自本地址域、宿于其它成员地址域的报文添加用以标识本地址域身份的“标签”，该标签可验证，确保地址域地址前缀不被冒用。

P87 控制层，P88 数据层，P89 状态机，P90 数据转发，P91 标签验证，P92 基于区块链的域间信任联盟。P94 标识格式和验证替代，P95 信任联盟与节点管理

P93 层次结构

SAVA-X分层：支持五层结构（不要求全部具备），自上而下为信任联盟、子信任联盟（CERNET/电信网）、一级（AS、地址域）/二级（院系）/三级（楼宇）地址域

基于 IPV6 的可信身份识别 P97~98

技术难点

- 网络的分布式管理与终端标识的跨域有效性间的矛盾
- 要求真实性标识基于统一结构

研究思路

- IPv6地址空间承载终端标识保障跨域验证的有效性

1. 在地址真实性的基础上，设计嵌入可信设备标识符的IPv6 地址生成算法，兼顾多种IPv6地址分 配机制和组网环境, 将端设备信息携带于数据包中，实现端网协同
2. 地址标识采用动态更新机制，达到对终端设备或终端用户的身份动态标识和隐私保护的目的
3. 构建可信设备标识符的认证、管理、追溯和审计机制

基于真实地址验证关键技术，通过在IP地址中嵌入可信设备标识符，实现了端网协同的真实用户身份识别和溯源，赋予地址防重放、防逆推、防DDoS等特性。

P99 数据包防篡改机制 P99~100

技术难点：SAVA体系结构保障源地址的真实性，确保数据包源地址可追溯、可验证。然而数据包在域间传递的过程中仍然存在数据内容被篡改的风险

研究思路：数据包完整性校验

针对数据包传输路径上可能存在的恶意篡改问题，提出数据包防篡改机制；验证效率高、复杂度低、部署结构可扩展性强、防篡改能力突出。

利用SAVA-X标签证明源端身份，增加数据包摘要信息共同生存数据包签名；中间节点不具有源端SAVA-X标签，无法伪造数据包签名，防止其它恶意节点篡改数据包。