真实源地址验证

- 设计背景 P8
  - 基于 IP 地址伪造的攻击 P11
  - 危害严重 P13
  - 现有防御方法 P15
  - 现有方法的缺陷 P16
    - 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
    - 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
    - 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。
    - 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
    - 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
  - 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
    - 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
  - 面向地址域的新型源地址验证SAVA体系结构 P51~52
    - 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
    - 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
  - 无线 SAVI P62
  - 802.1x 认证 P63
  - 动态自适应的地址分配分组监听 P64~65
  - SAVI 技术方案概要 P66
    - 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
    - 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
  - 原地址验证表 SAVA-P P68
  - 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
  - DPP 报文的生成与处理 P74~85
  - 方案总结 P85
  - 域间真实源地址验证 SAVA-X P86
  - P93 层次结构
  - 基于 IPV6 的可信身份识别 P97~98
    - 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
    - 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
  - P99 数据包防篡改机制 P99~100