OpenFlow+ for IPv6 Source Address Validation

Jun Bi
Tsinghua University, China
Source Address Validation (SAV)

- Why SAV
  - The current Internet architecture: packet forwarding is only based on destination address
    - Issues: attacks by address spoofing, management....
  - SAV will be good for:
    - anti-spoofing/network security
    - network management/traceback
    - network measurement
    - network accounting/billing
Source Address Validation (SAV)

- IETF SAVI WG
  - Solutions for SAV at the first hop
  - Especially for IPv6
- Why SAV beyond the first hop is tough
  - Asymmetric Routing, ECMP
  - uRPF only makes filtering decision based on local FIB, may cause false positive
- What Tsinghua proposed and implemented
  - CPF (Calculation based forwarding) to make filtering decision based on global FIBs
  - A central control model is feasible in the Intra-AS scenario
CPF at Intra-AS

- A CPF controller collects the FIBs of every router inside an AS, then calculates all possible forwarding paths for every source prefix, and generates the filter table for each router.
- Spoofing alarm based on sampled packets, then downloads ACLs into routers.
Protocols used in CPF

- **SNMP**
  Polling the forwarding table, interface table, and subnet information from MIB agent in the router

- **xFlow** (NetFlow/sFlow)
  Sampling packets from the router through xFlow for spoofing alarm.

- **Telnet/SSH**
  Configuring the ACL into routers remotely to filter spoofing traffic
Limitations of CPF

-The router control interface is not fully standardized
  - CLI is not standardized - have to design different telnet scripts for different vendors
  - ACL format is not standardized - have to design different ACLs for different vendors

-The router can not be easily controlled from outside
  - The communication between CPF and router is inefficient. The routing table changes can not be reported to CPF in real-time, so may cause false-positive when topology changes
  - Telnet/CLI scripts can not be smart enough to handle all situations of ACLs updates
OpenFlow

OpenFlow Switch

Secure Channel

Flow Table

Controller

PC

OpenFlow Switch specification

OpenFlow Protocol

SSL

The Stanford Clean Slate Program

http://cleanslate.stanford.edu
What OpenFlow brings to us

• OpenFlow enables network innovation, by:
  - FlowTable in the device and OpenFlow protocol between controller and device implement the standardization and open access of network device.
  - User-defined new protocols can be easily added to the controller as new components.
  - The centralized mode in OpenFlow makes functions based on global information possible.
What OpenFlow brings to us

- Open and standard new protocol deployment
- Open and standard control interfaces
- Open and standard hardware interfaces

Diagram:
- Hardware to OpenFlow
- Device
- Hardware
- OpenFlow Protocol
- Control Protocol
CPF and Openflow

- Central control architecture of OpenFlow matches CPF, which requires global information of an AS
- Using OpenFlow protocol to unify three protocols used by CPF (SNMP, xFlow and Telnet) for communications between CPF controller and network devices
- Efficient control from outside the network device to minimize the false positive/false negative of CPF
Challenges of Current OpenFlow

• To adapt all future protocols and different vendors -- needs the flow table more open
• When a protocol becomes mature enough -- needs the controller/app inside the device to improve the efficiency and performance
• To have OpenFlow working in the inter-domain scenario – needs to design inter-domain coordination channel
• To make deployment low-cost and deployable -- Needs to implement OpenFlow in today’s router
Openflow+

• Openflow+ is an extension to the fundamental architecture of OpenFlow to make it more open, efficient, deployable, and low-cost:
  - 1: Flow Table Extension
  - 2: Control Mode Extension
  - 3: Inter-Domain Extension
  - 4: OpenRouter (Low-cost Openflow for today’s router)
Extension 1: Flow Table Extension

Flow Table

Mandatory

Optional

Vendor-defined

Hardware to OpenFlow Protocol

Device Hardware OpenFlow Protocol Control Protocol
Extension 2: Distribution Mode Extension

Flow Table

Hardware to OpenFlow
Protocol to OpenFlow
Protocol to Protocol

Device Hardware OpenFlow Protocol Control Protocol
Extension 3: Inter-Domain Extension

![Diagram showing the interaction between Hardware and OpenFlow Protocol through Flow Tables and Control Protocols.]
Extension 4: Low-cost Openflow for today’s router (OpenRouter)

- OpenFlow in a commercial router
  - DCRS 5980/5950, DigitalChina Company
Extension 4: Low-cost Openflow for today’s router
Architecture of CPF based on OpenFlow+
CPF Controller Implementation

CPF APP

Filtering Rule | Validation Module | Rule Adaptor

Generator

NOX

Network State | Sampling Packet

Processor | Processor

OR OpenRouter

OpenFlow

Sharing Memory

Socket

OR A

OR B

OR C

OR D

OR E

OR F

OR G
The Testbed of CPF based on OpenFlow+
Thanks!