Gap Analysis, Problem Statement and Requirements for Source Address Validation in Intra-domain Networks

Dan Li, Jianping Wu, Lancheng Qin, Mingqing Huang, Nan Geng

Mar 29, 2023

Background

- Goals
  - Perform the gap analysis of existing intra-domain SAV mechanisms
  - Summarize the fundamental problems of existing intra-domain SAV mechanisms
  - Describe the requirements for new intra-domain SAV mechanisms
- Historical versions
  - **draft-li-savnet-intra-domain-problem-statement-00, IETF 114 SAVNET WG**
  - draft-li-savnet-intra-domain-problem-statement-01, Sep 25, 2022
  - draft-li-savnet-intra-domain-problem-statement-02, Oct 22, 2022
  - **draft-li-savnet-intra-domain-problem-statement-03, IETF 115 SAVNET WG**
  - draft-li-savnet-intra-domain-problem-statement-04, Nov 30, 2022
  - draft-li-savnet-intra-domain-problem-statement-05, Dec 15, 2022
  - draft-li-savnet-intra-domain-problem-statement-06, Feb 23, 2023
  - **draft-li-savnet-intra-domain-problem-statement-07, IETF 116 SAVNET WG**

Comments on Version-03

- Barry Greene: The impact of DOCSIS tools for SAV, TR-69 and FTTH tools for SAV, and DHCP Source Verify tools should be included in the Introduction section.
  - Response: They are all access network SAV tools. The updated draft introduces existing access network SAV tools and makes it clear that they are not the focus of SAVNET WG.
- Roland Dobbins: Should we focus on inter domain instead of intra domain?
  - Response: Both are in the scope of SAVNET WG. The updated draft describes the boundary between intra-domain and inter-domain SAV.
- Anthony: Why removed the part for misaligned incentive from intra-domain draft? Incentive problem is not technical, but a commercial one.
  - Response: First, incentive is actually a technical problem, i.e., the deployed AS can benefit from deployment. Second, incentive is mainly for inter-domain SAV. Third, we put incentive problem to an individual draft.

Comments on Version-03

- Jared Mauch: SAV may break more things than it can preventing, because the largest attack today doesn't come from spoofed packets.
  - Response: SAV is important for identifying and preventing various spoofing-based attacks. That is why communities (e.g., ISOC) and organizations (e.g., CAIDA) care much about the deployment of SAV. In recent years, the DDoS reports published by NetScout [1] and Cloudflare [2] have indicated that a significant proportion of DDoS attacks are based on source address spoofing.
- Jared Mauch: There are completely impossible things such as the entirety of 3.2 which must be striken in order to have a point to start with.
  - Response: It is worth of more discussion. The updated draft reframes the Requirement section to put requirements as which can be fully or partially fulfilled when designing new intra-domain SAV mechanisms.

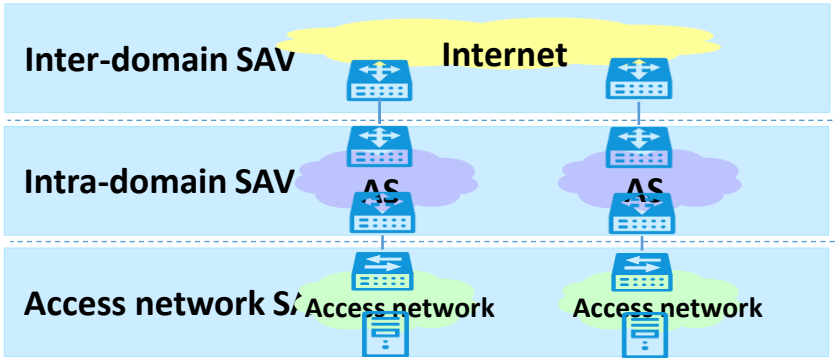
[1] DDoS THREAT INTELLIGENCE REPORT. https://www.netscout.com/threatreport/
[2] Cloudflare DDoS threat report for 2022 Q4. https://blog.cloudflare.com/ddos-threat-report-2022-q4/

Main Updates Compared to Version-03

- Updates in Introduction section
  - Introduce access-network SAV mechanisms
  - Goals of intra-domain SAV mechanisms
- A new Existing Mechanism section
- Updates in Gap Analysis section
- Updates in Problem Statement section
- Updates in Requirements section

Introduce Access Network SAV Mechanisms

- SAVA architecture [RFC 5210] divides SAV into three checking levels
  - Access network SAV, intra-domain SAV, inter-domain SAV



- Access network SAV ensures that a host uses a legitimate source IP address
  - Such as Static ACL, Dynamic ACL (e.g., RADIUS and DIAMETER), SAVI [RFC7039], SAVI solution for DHCP [RFC7513], IP Source Guard (IPSG), Cable Source-Verify
  - Not the main focus of SAVNET WG
- Access network SAV is not enough
  - Given numerous access networks managed by different operators in the Internet, it is difficult to require all access networks to deploy SAV
  - When some access networks do not deploy SAV, intra-domain and inter-domain SAV at routers can help block spoofing traffic as close to the source as possible
  - The main focus of SAVNET WG; IP-prefix-level instead of IP-address-level

Boundary between Intra-domain and Inter-domain SAV Mechanisms

Intra-domain SAV mechanisms

- An AS X defends against source address spoofing without the collaboration of other Ases (without information from other ASes)
  - Goal 1: prevent the outgoing traffic originated from a subnet of AS X from spoofing the addresses of other subnets
  - Goal 2: prevent the incoming traffic to AS X from spoofing the addresses of AS X

Inter-domain SAV mechanisms

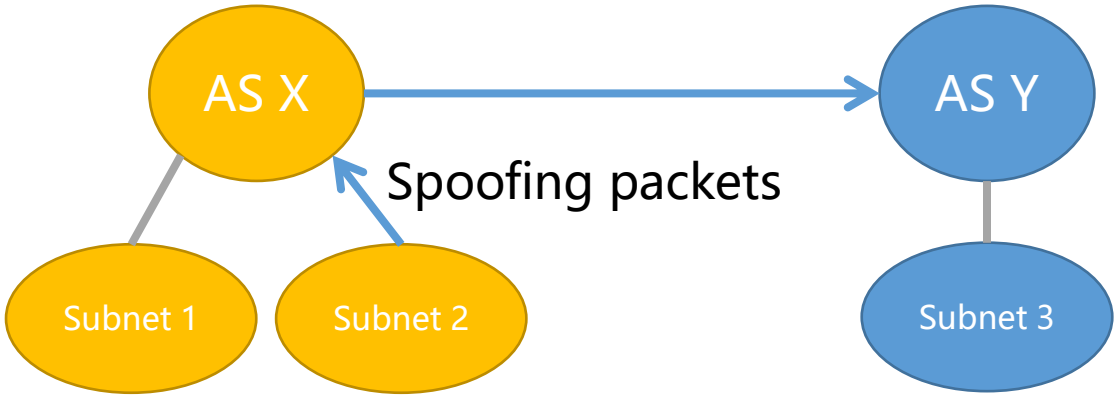
- Multiple ASes collaborate with each other for defending against source address spoofing (with information exchange between ASes)
  - An intermediate AS X helps defend against spoofing traffic originated from AS A which spoofs the addresses of AS B

Goals of Intra-domain SAV Mechanisms

- The intra-domain SAV for AS X has two goals:
  - Goal #1: outbound traffic validation
    - block the illegitimate packets originated from the local subnets of AS X which spoof the addresses of other subnets (either within the AS or other ASes)

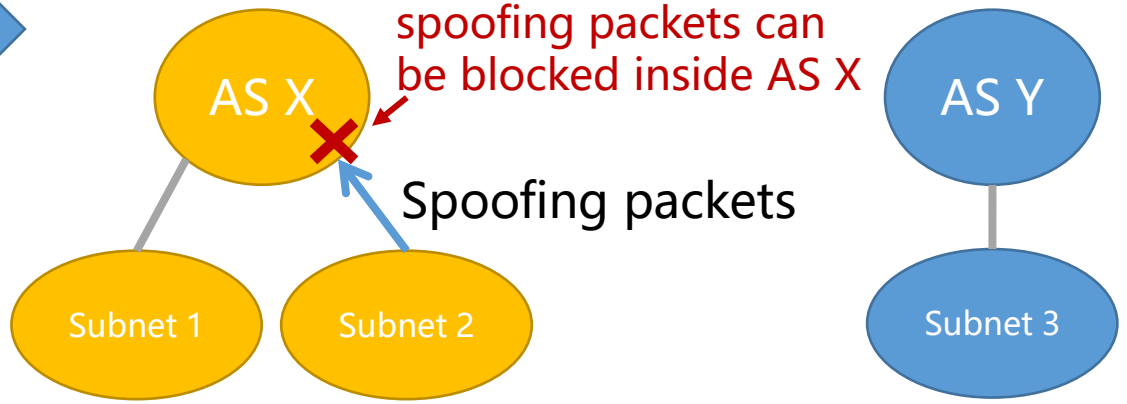
Case #1

Subnet 2 of AS X sends packets which spoof the addresses of subnet 1 or 3



Goal #1

If AS X deploys intra-domain SAV, the spoofing packets can be blocked inside AS X

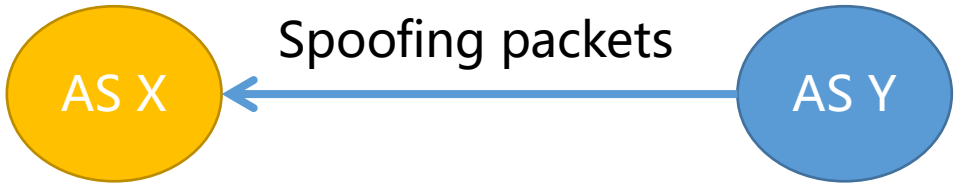


Function of Intra-domain SAV

- The intra-domain SAV for AS X has two goals:
  - Goal #1: outbound traffic validation
    - block the illegitimate packets originated from the local subnets of AS X which spoof the addresses of other subnets (either within the AS or other ASes)
  - Goal #2: inbound traffic validation
    - block the illegitimate packets coming from other ASes which spoof the source addresses of AS X

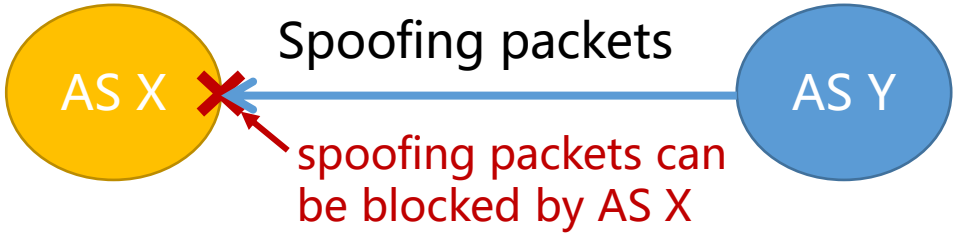
Case #2

AS X receives incoming packets which spoof AS X's addresses



Goal #2

If AS X deploys intra-domain SAV, the spoofing packets can be blocked by AS X



Main Updates Compared to Version-03

- Updates in Introduction section
- A new Existing Mechanism section
  - ◆Add more details about analyzing existing intra-domain SAV mechanisms
- Updates in Gap Analysis section
- Updates in Problem Statement section
- Updates in Requirements section

Existing Intra-domain SAV mechanisms

Ingress filtering [RFC2827, RFC3704] is the current practice of intra-domain SAV

- ACL-based SAV [RFC2827, RFC3704]
- Strict uRPF [RFC3704]
- Loose uRPF [RFC3704]
- Carrier Grade NAT

ACL-based SAV [RFC2827, RFC3704]

- Working principle
  - ACL rules can be configured for blocking or permitting packets with specific source addresses
- ACL-based SAV can work for both outbound traffic validation and inbound traffic validation
  - For outbound traffic validation
    - Applied at the downstream interfaces of edge routers connecting the subnets or at the downstream interfaces of aggregation routers
  - For inbound traffic validation
    - Applied at the upstream interfaces of routers connecting other ASes
- In any application scenario, ACL rules should be manually updated in time to be consistent with the latest filtering criteria

Strict uRPF [RFC3704]

- Working principle
  - The packet is permitted only when i) the local FIB contains a prefix encompassing the packet's source address, and ii) the corresponding outgoing interface for the prefix in the FIB matches the packet's incoming interface
- Strict uRPF usually works for outbound traffic validation
  - Applied at downstream interfaces of edge routers connecting local subnets
- Strict uRPF can generate and update SAV rules automatically, but has serious improper block problems in the scenario of asymmetric routing

Loose uRPF [RFC3704]

- Working principle
  - The packet is permitted if the local FIB contains a prefix encompassing the packet's source address
- Loose uRPF usually works for inbound traffic validation
  - Applied at upstream interfaces of routers connecting other ASes
- Loose uRPF can generate and update SAV rules automatically, but most spoofing packets will be improperly permitted

Carrier Grade NAT

- Working principle
  - If the source address of a packet is in the INSIDE access list, the NAT rule can translate the source address to an address in the pool OUTSIDE
- Carrier Grade NAT has some operations on source addresses of packets, but is not an anti-spoofing tool, as described in the MANRS Implementation Guide
  - The NAT rule cannot judge whether the source address is spoofed or not
  - The packet with a spoofed source address will be forwarded directly if the spoofed source address is not included in the INSIDE access list

Main Updates Compared to Version-03

- Updates in Introduction section
- A new Existing Mechanism section
- Updates in Gap Analysis section
  - Outbound traffic validation
  - Inbound traffic validation
- Updates in Problem Statement section
- Updates in Requirements section

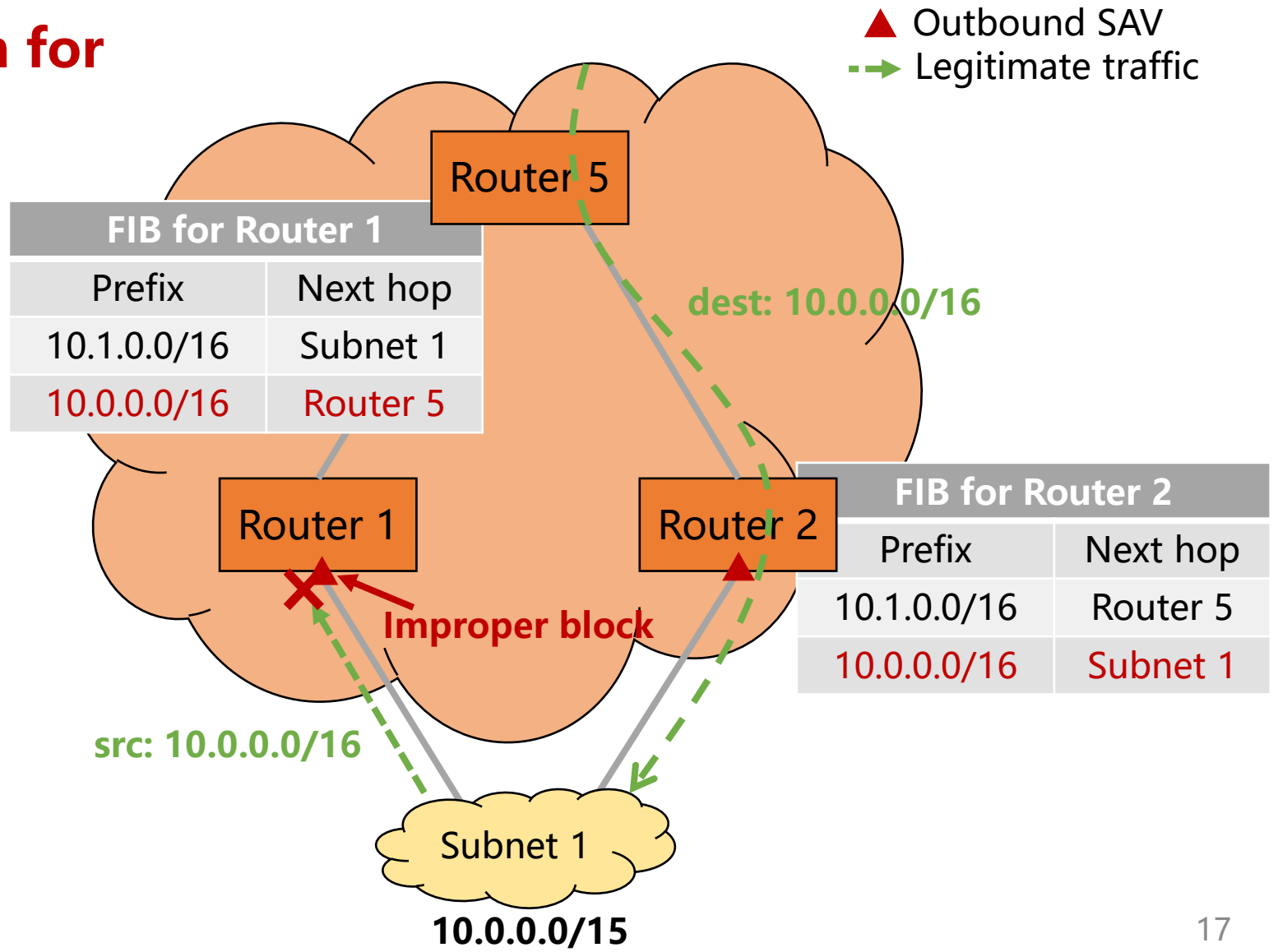
Outbound Traffic Validation

Outbound traffic validation for multi-homed subnet

- Router 1 only advertises 10.1.0.0/16 in IGP
- Router 2 only advertises 10.0.0.0/16 in IGP

Behavior

- If applying ACL-based SAV
  - Manual update given prefix or topology update in Subnet 1
- If applyiing strict uRPF
  - Improper block



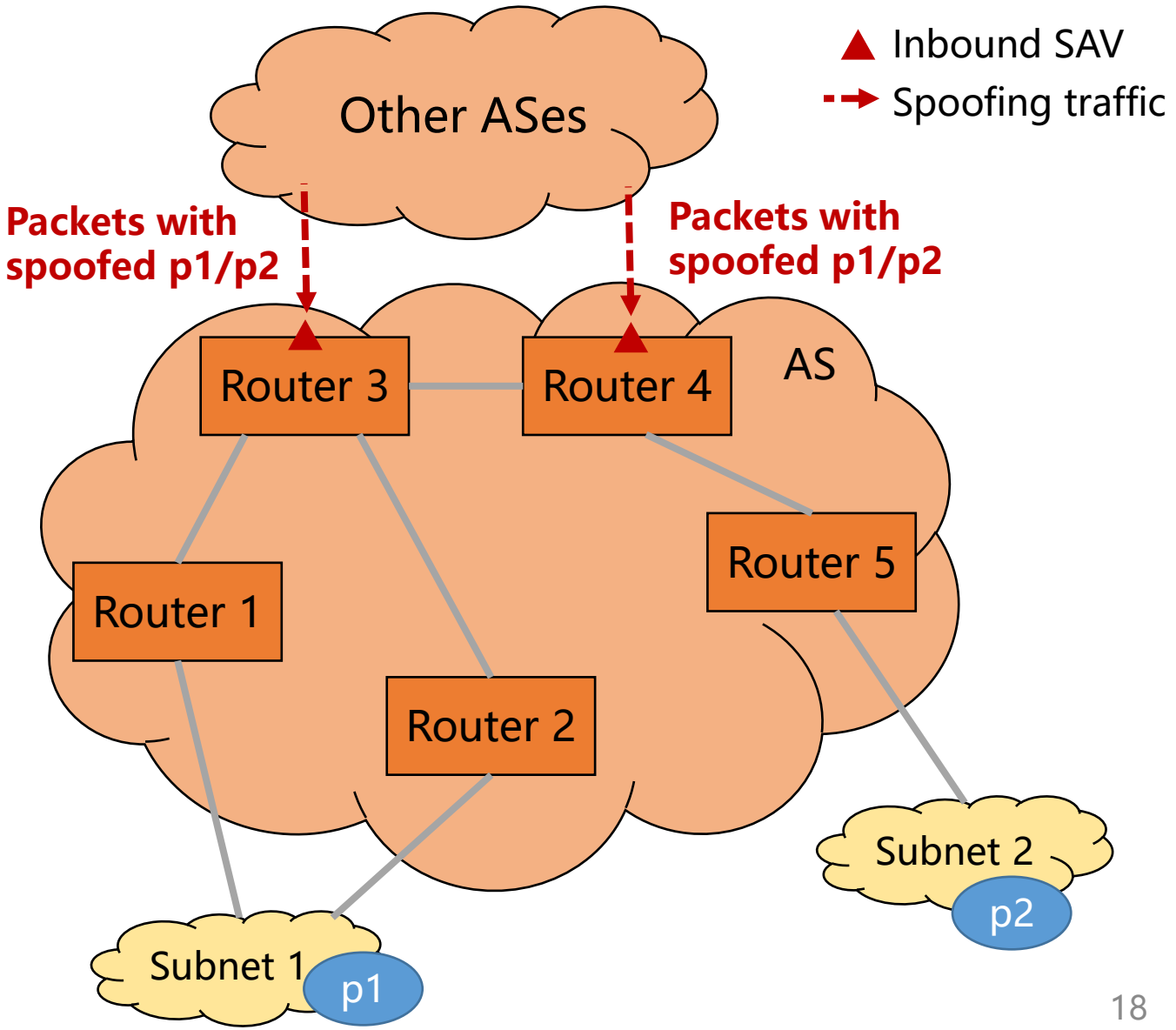
Inbound Traffic Validation

Inbound traffic validation

- Block inbound packets with internal source addresses at upstream interfaces

Behavior

- If applying ACL-based SAV
  - Manual update when internal prefixes or network topology change dynamically
- If applying loose uRPF
  - Large amount of improper permit



Main Updates Compared to Version-03

- Updates in Introduction section
- A new Existing Mechanism section
- Updates in Gap Analysis section
- Updates in Problem Statement section
  - ◆Remove the problem of “limited protection”
  - ◆Summarize the problem for each intra-domain SAV mechanism
- Updates in Requirements section

Problem Statement

- ACL-based SAV
  - Problem: high operational overhead
  - Reason: requiring manual update when network topology, IP prefix or routing rule changes
- Strict uRPF
  - Problem: improper block under asymmetric routing
  - Reason: conducting SAV based on local FIB which may not match the real data-plane forwarding path from the source
- Loose uRPF
  - Problem: large amount of improper permit
  - Reason: allowing packets with source addresses that exist in the FIB table at all router interfaces

Main Updates Compared to Version-03

- Updates in Introduction section
- A new Existing Mechanism section
- Updates in Gap Analysis section
- Updates in Problem Statement section
- Updates in Requirements section
  - ◆Add the requirement of “working in Incremental/Partial Deployment”
  - ◆Revise the description of other requirements

Requirements for New Intra-domain SAV Mechanisms

The requirements can be fully or partially fulfilled when designing new intra-domain SAV mechanisms

- Requirement #1: The mechanism MUST support automatic update
  - Automatically adapt to network dynamics instead of relying on manual update
- Requirement #2: The mechanism MUST improve the validation accuracy
  - Avoid improper block under asymmetric routing
    - Must include the real forwarding path in the data plane
  - Reduce improper permit as much as possible
    - By including the real forwarding path in the data plane, minimize the set of permittable paths
- Requirement #3: The mechanism SHOULD work in incremental/partial deployment
  - Provide effective protection when partially deployed in the intra-domain network

Acknowledgements

Many thanks to the valuable comments from:

- Jared Mauch, Barry Greene, Fang Gao, Anthony Somerset, Kotikalapudi Sriram, Yuanyuan Zhang, Igor Lubashev, Alvaro Retana, Joel Halpern, Aijun Wang, Michael Richardson, Li Chen, Gert Doering, Mingxing Liu, Libin Liu, John O'Brien, Roland Dobbins, etc.

Thanks!