Source Address Validation in Inter-domain Networks (Inter-domain SAVNET) Gap Analysis, Problem Statement, and Requirements

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

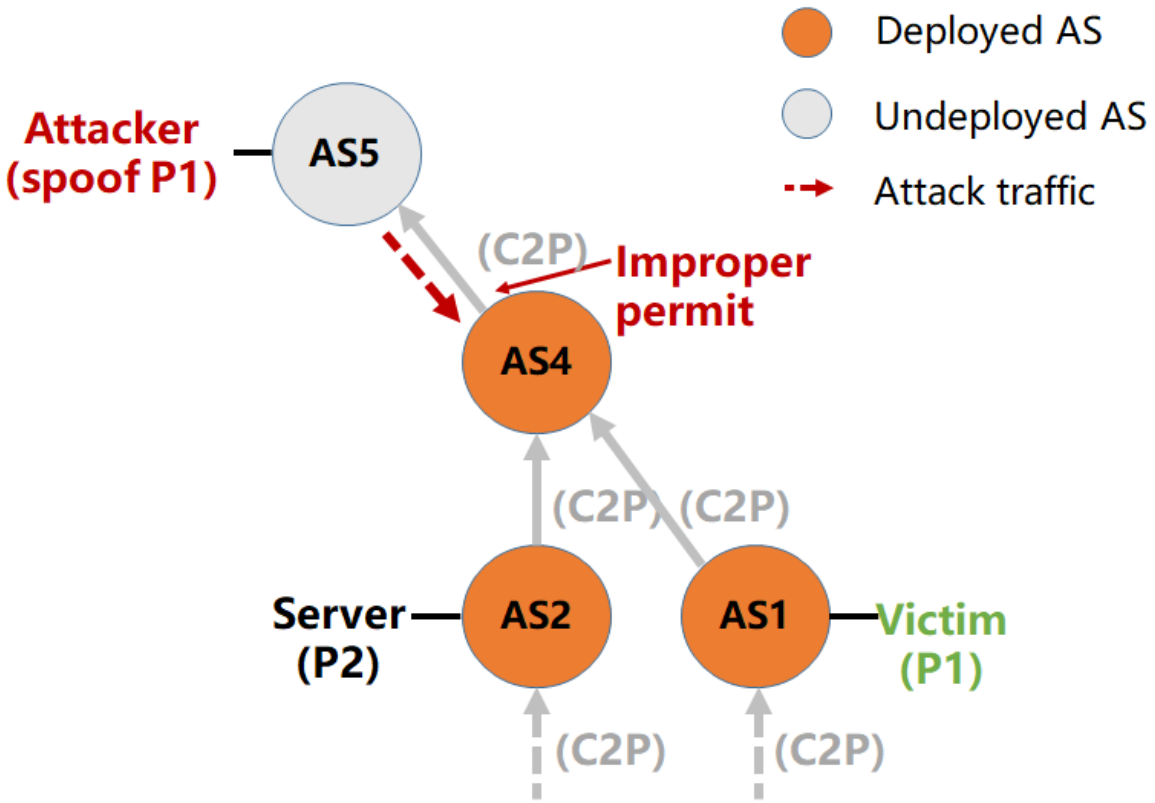
Nov 11, 2022

Background

- Goals
  - Provide the gap analysis of existing inter-domain SAV mechanisms
  - Summarize the fundamental problems of existing inter-domain SAV mechanisms
  - Define the requirements for the new inter-domain SAV mechanism
- Versions
  - draft-wu-savnet-inter-domain-problem-statement-00, IETF 114 SAVNET WG
  - draft-wu-savnet-inter-domain-problem-statement-01, Sep 25, 2022
  - draft-wu-savnet-inter-domain-problem-statement-02, Oct 22, 2022
  - draft-wu-savnet-inter-domain-problem-statement-03, IETF 115 SAVNET WG

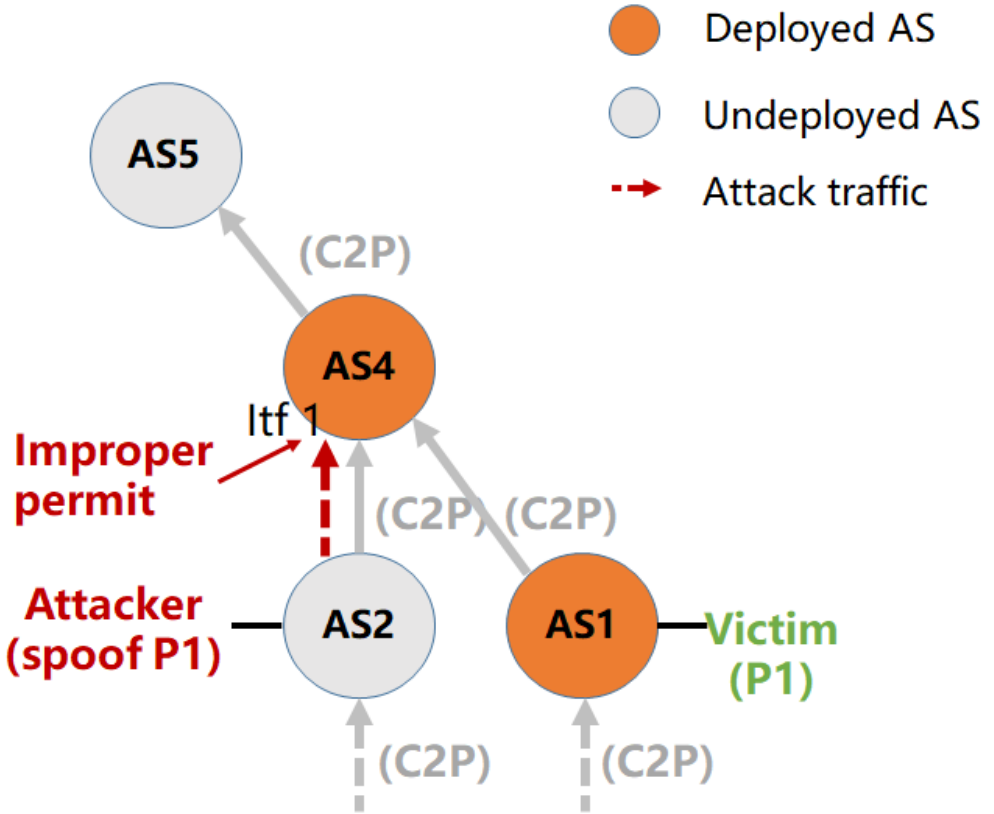
Gap Analysis in Version-00

Scenario #1: Reflection attack



Scenario 1: Reflection attack

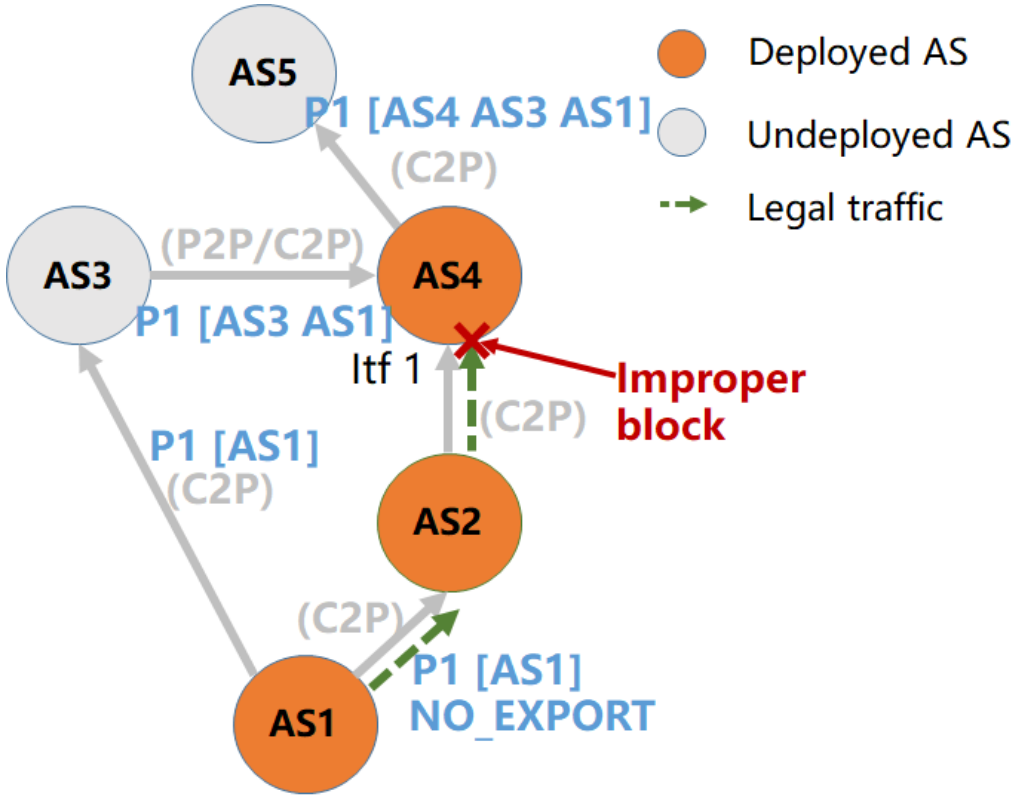
Scenario #2: Spoofing within the customer cone



Scenario 2: Spoofing within a customer cone

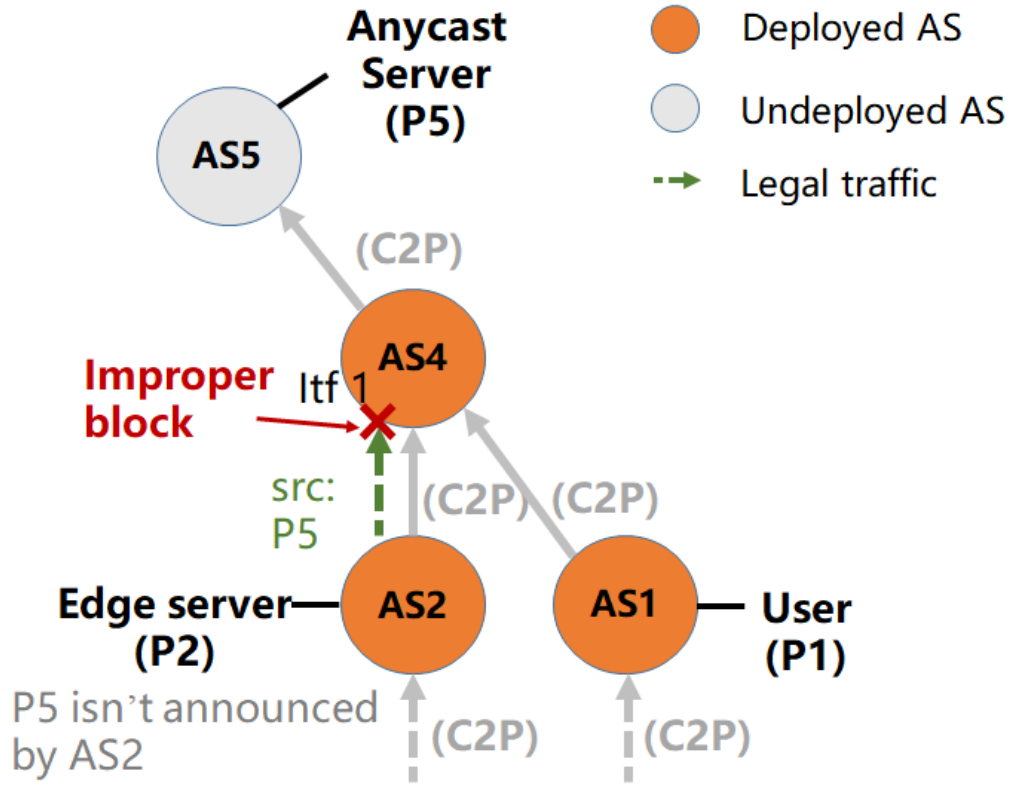
Gap Analysis in Version-00

Scenario #3: NO_EXPORT in BGP advertisement



Scenario 3: NO_EXPORT in BGP Advertisement

Scenario #4: Direct Server Return (DSR)



Scenario 4: Direct Server Return (DSR)

21

Comments on Version-00

Version-00

1. Introduction . . . . . .
2. Terminology . . . . . .
3. Gap Analysis . . . . . .
   3.1. Weak Downstream Checking . . . . . .
   3.2. Underperforming Upstream Checking . . .
      3.2.1. NO_EXPORT in BGP Advertisement . .
      3.2.2. Spoofing within Customer Cone . . .
      3.2.3. Direct Server Return (DSR) Scenario
4. Problem Statement . . . . . .
   4.1. Limitation in Accuracy . . . . . .
   4.2. Misaligned Incentive . . . . . .
5. Requirements . . . . . .
   5.1. Accurate Path Discovery . . . . . .
   5.2. All-round Protection . . . . . .
   5.3. Incremental Deployment and Incentive .
6. Security Considerations . . . . . .
7. Acknowledgments . . . . . .
8. Normative References . . . . . .
Authors' Addresses . . . . . .

- How is misaligned Incentive different from improper permit?
- What incentive does SAVNET hope to achieve?
- Are we talking about non-IP packets as well?
- ……

Main Updates Compared to Version-00

- Updates in problem statement
  - Improve the description of misaligned incentive
- Updates in requirements
- Two new sections

Misaligned Incentive

Misaligned incentive is one of the main reasons why some ASes have not yet deployed BCP38

"Commonly referred to as "Source Address Validation" (SAV) or Best Current Practice (BCP) 38, this prophylactic only prevents a provider who deploys SAV from originating spoofed-source traffic; it does not protect the provider from receiving spoofed traffic or being the victim of an attack. Unfortunately, continual incidences of spoofing demonstrates that SAV is not ubiquitously deployed"

Reference: Network Hygiene, Incentives, and Regulation: Deployment of Source Address Validation in the Internet. Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. 2019

"The benefits of implementing SAV flow to the rest of the Internet, not the operators themselves. The network implementing SAV is still vulnerable to DDoS attacks from other networks"

Reference: Deployment of Source Address Validation by Network Operators: A Randomized Control Trial. IEEE Symposium on Security and Privacy (S&P). 2022

"Due to incentive misalignments, the adoption of SAV has been slow and a recent study found that many ASes still do not employ it in their networks"

Reference: PISKES: Pragmatic Internet-Scale Key-Establishment System. Proceedings of the 15th ACM Asia Conference on Computer and Communications Security. 2020

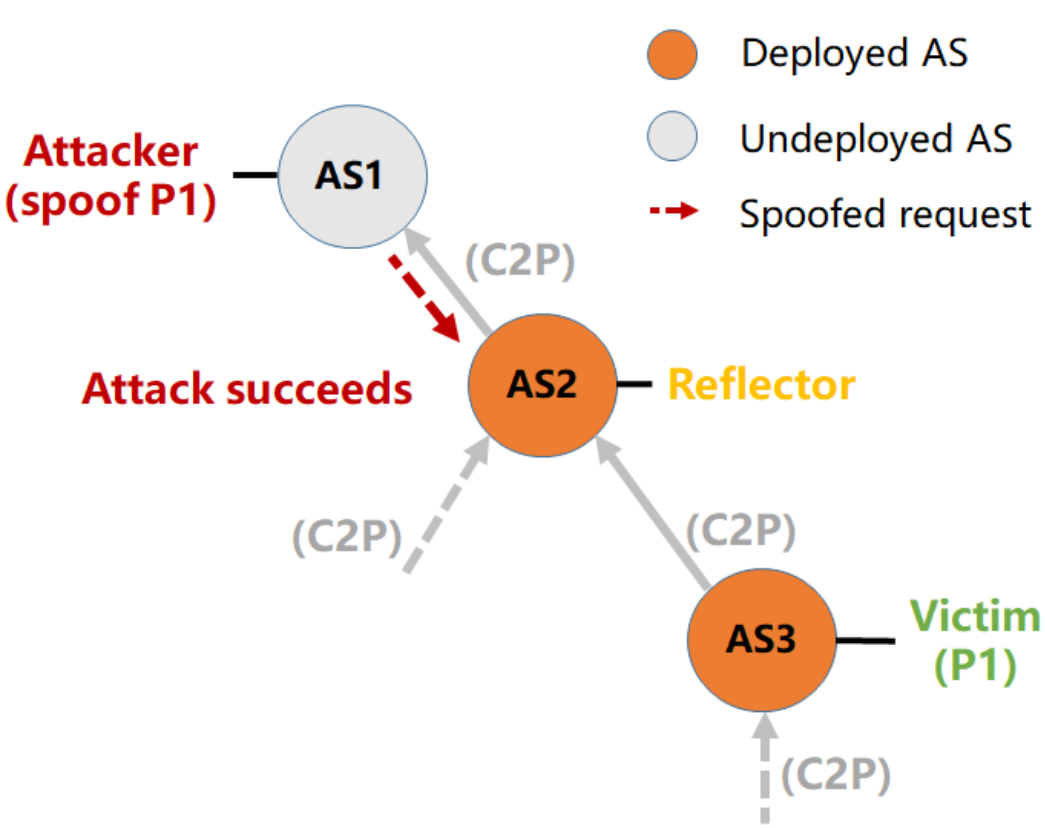
Misaligned Incentive

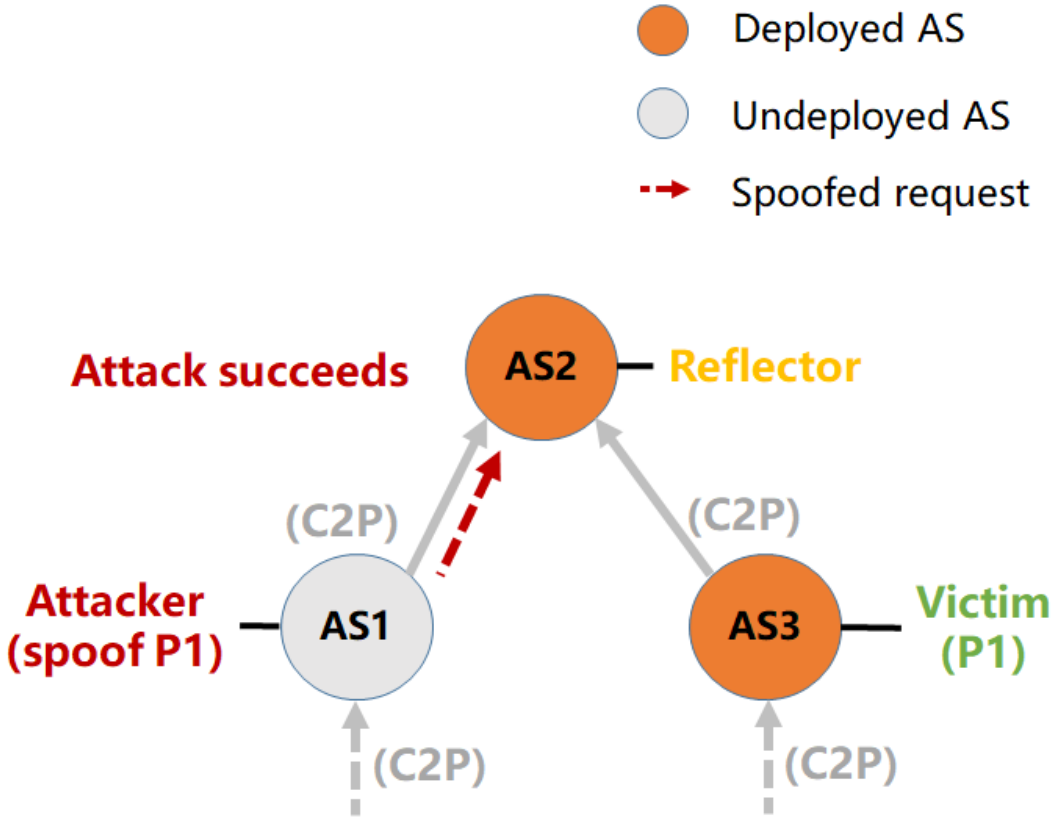
- Compared to BCP38, EFP-uRPF protects deployed AS from receiving spoofed traffic from customer interfaces
- However, EFP-uRPF is not well-aligned with market demand
  - It only prevents customer cone from originating spoofed traffic, but does not protect customer cone from receiving spoofed traffic from outside customer cone
  - An AS does not gain additional defense against reflection attacks by deploying EFP-uRPF

Reference: draft-qin-savnet-incentive. SAVNET's Incentive for Defense Against Reflection Attacks.

Misaligned Incentive

Behavior: Though **AS3 (victim)** and **AS2 (victim's upstream provider)** deploy SAV, the **reflection attacks succeed**





Reference: draft-qin-savnet-incentive. SAVNET's Incentive for Defense Against Reflection Attacks.

Problem Statement

- Problem #1: Inaccurate validation
  - Behavior gap: improper block or improper permit
  - Reason: conducting SAV based on local RIB which may not match the real data-plane forwarding path from the source
- Problem #2: Misaligned incentive
  - Behavior gap: suffering reflection attack even when SAV mechanisms have been deployed by victim
  - Reason: victim with SAV deployment does not participate in protecting its source addresses from being forged

Main Updates Compared to Version-00

- Updates in problem statement
- Updates in requirements
  - Revise the description of requirements
- Two new sections

Requirements for New Inter-domain SAV Mechanism

- Requirement #1: The mechanism MUST ensure accurate SAV
  - Match real data-plane forwarding path
  - Avoid improper block and reduce improper permit as much as possible
- Requirement #2: The mechanism MUST provide direct incentive
  - Validate traffic from all directions
  - Help the deployed AS mitigate reflection attacks
- Requirement #3: The mechanism MUST support incremental deployment
  - Prevent source address spoofing when partially deployed
- Requirement #4: The mechanism MUST not induce much overhead
  - Avoid data-plane packet modification
  - Limit the number of control-plane protocol messages

Main Updates Compared to Version-00

- Updates in gap analysis
- Updates in problem statement
- Updates in requirements
- Two new sections
  - ◆Inter-domain SAVNET work scope
  - ◆Security considerations

Two new sections

- Inter-domain SAVNET work scope
  - All IP-encapsulated scenarios are in scope
    - including both IPv4 and IPv6 addresses
  - Non-IP packets are out of scope
- Security considerations
  - SAVNET focuses on routing protocol-based mechanisms, so the security scope of inter-domain SAVNET should be similar to that of BGP
    - If the new inter-domain SAV mechanism requires control-plane information exchange, there should be security considerations on the avoidance of message alteration or message injection

Thanks!

Backup slides

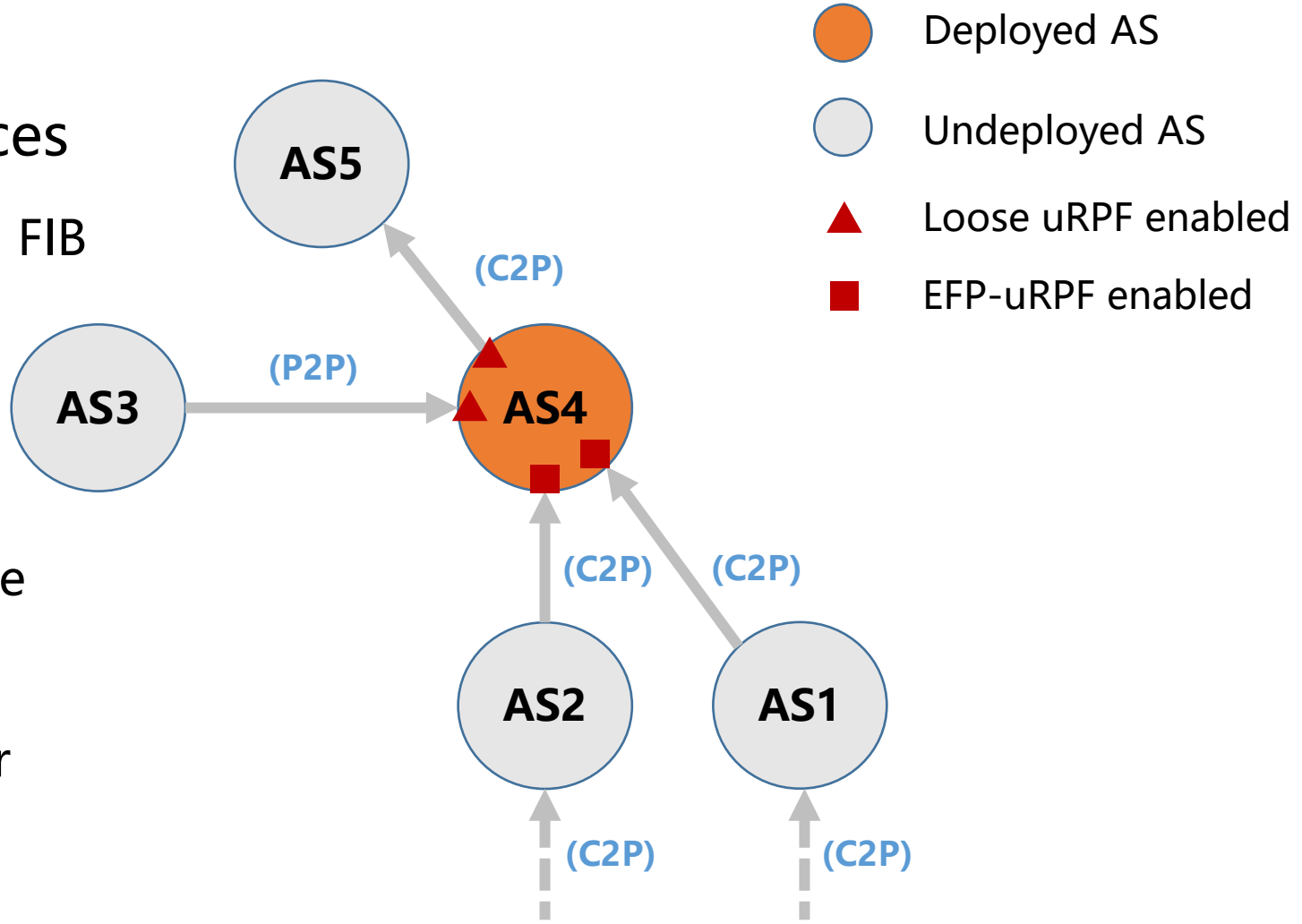
Typical Adoption of Inter-domain SAV

Loose uRPF

- Works on provider/peer interfaces
  - Accepts source addresses existing in FIB

EFP-uRPF

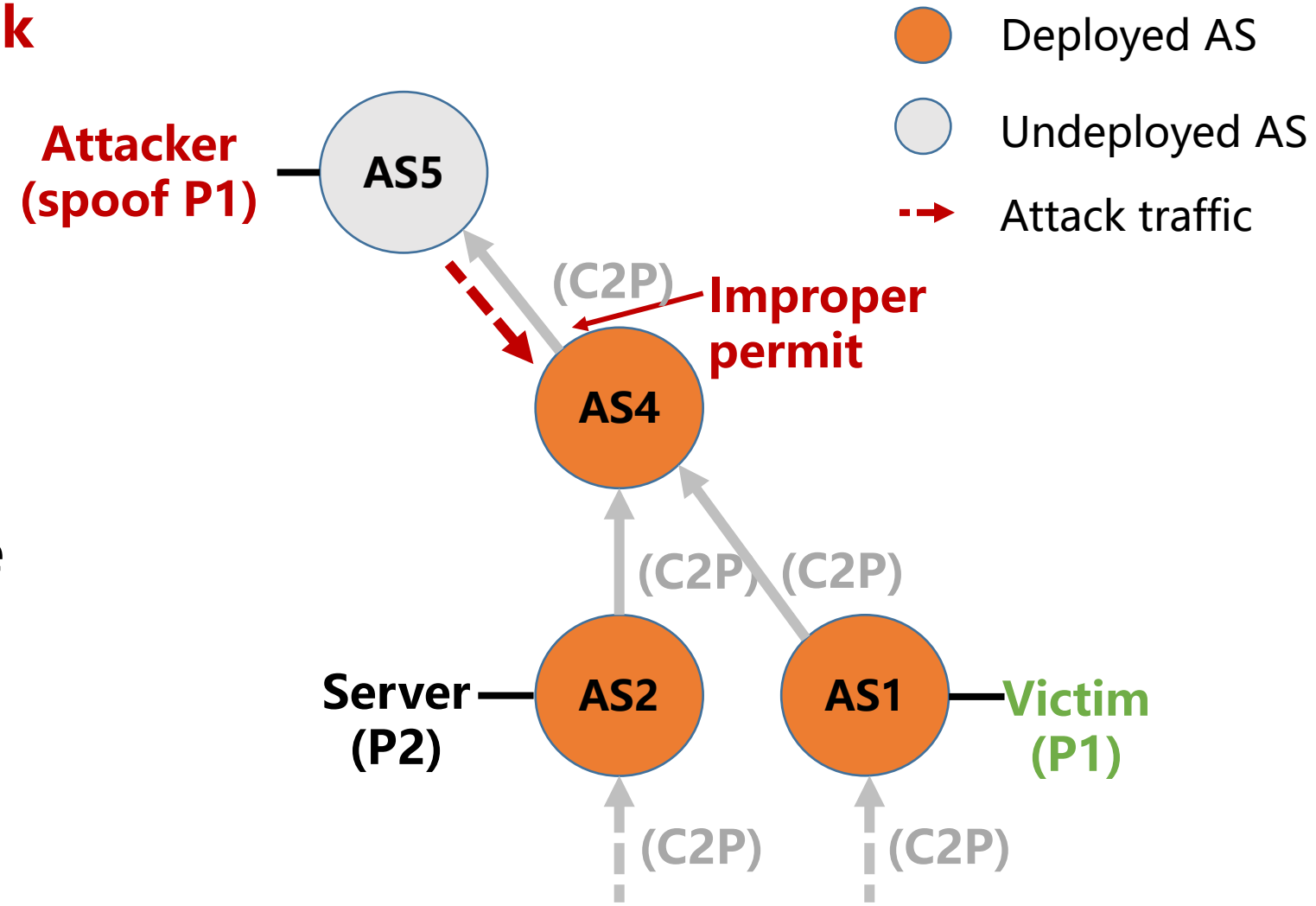
- Works on customer interfaces
  - Algorithm A: each customer interface applies an individual RPF list
  - Algorithm B (preferred): all customer interfaces share a same RPF list



Gap #1: Improper Permit

Scenario 1: Reflection attack

- Attacker: AS5
- Reflective server: AS2
- Victim: AS1



Scenario 1: Reflection attack

Behavior

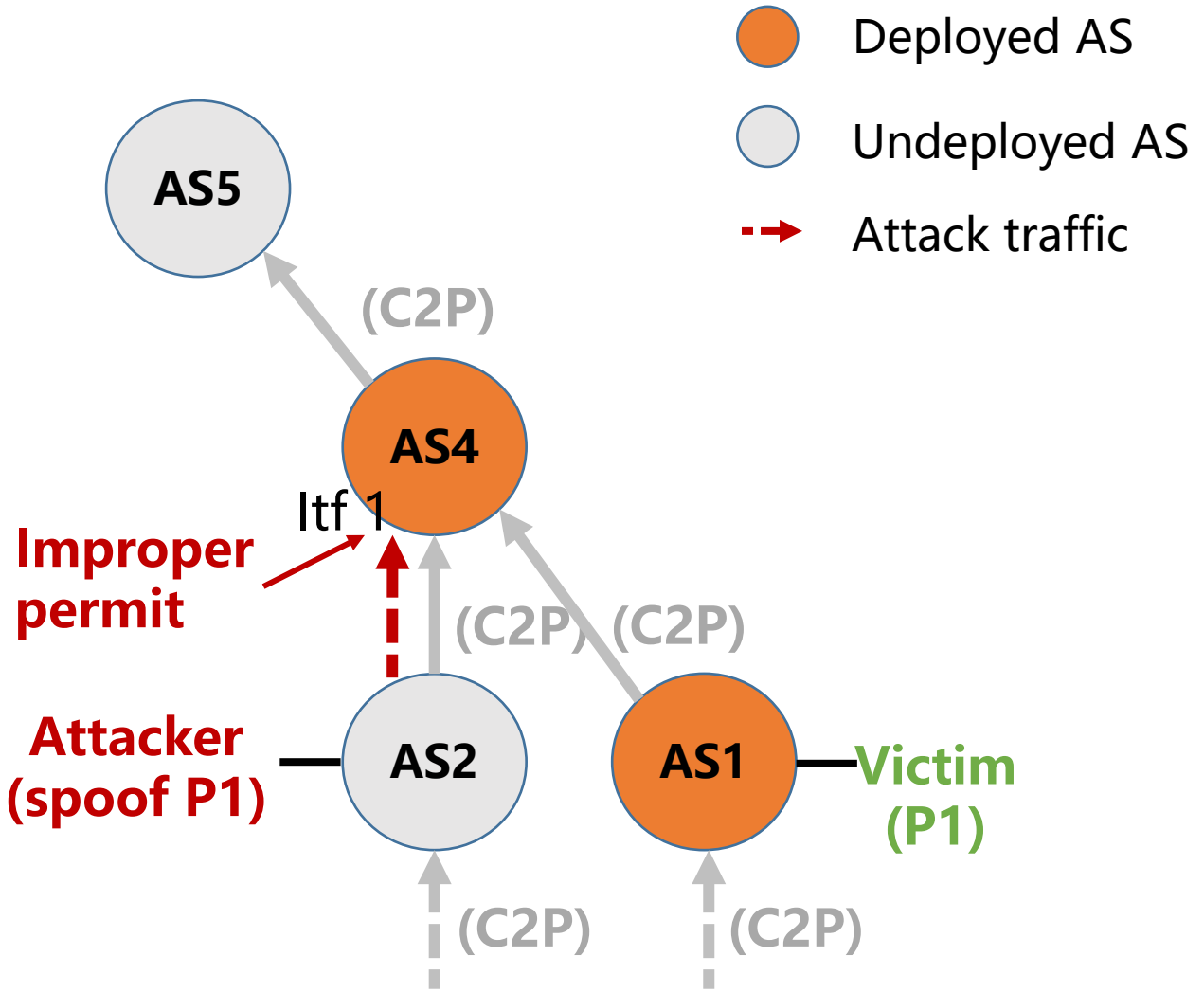
- AS4 **improperly permits** the spoofing traffic from AS5
  - Loose uRPF almost accepts any source address

Gap #1: Improper Permit

- **Scenario 2: Spoofing within the customer cone**

Behavior

- If AS4 runs EFP-uRPF Algorithm A
  - ◆Works well
- If AS4 runs EFP-uRPF Algorithm B
  - ◆**Improper permit** at Itf 1



Scenario 2: Spoofing within a customer cone

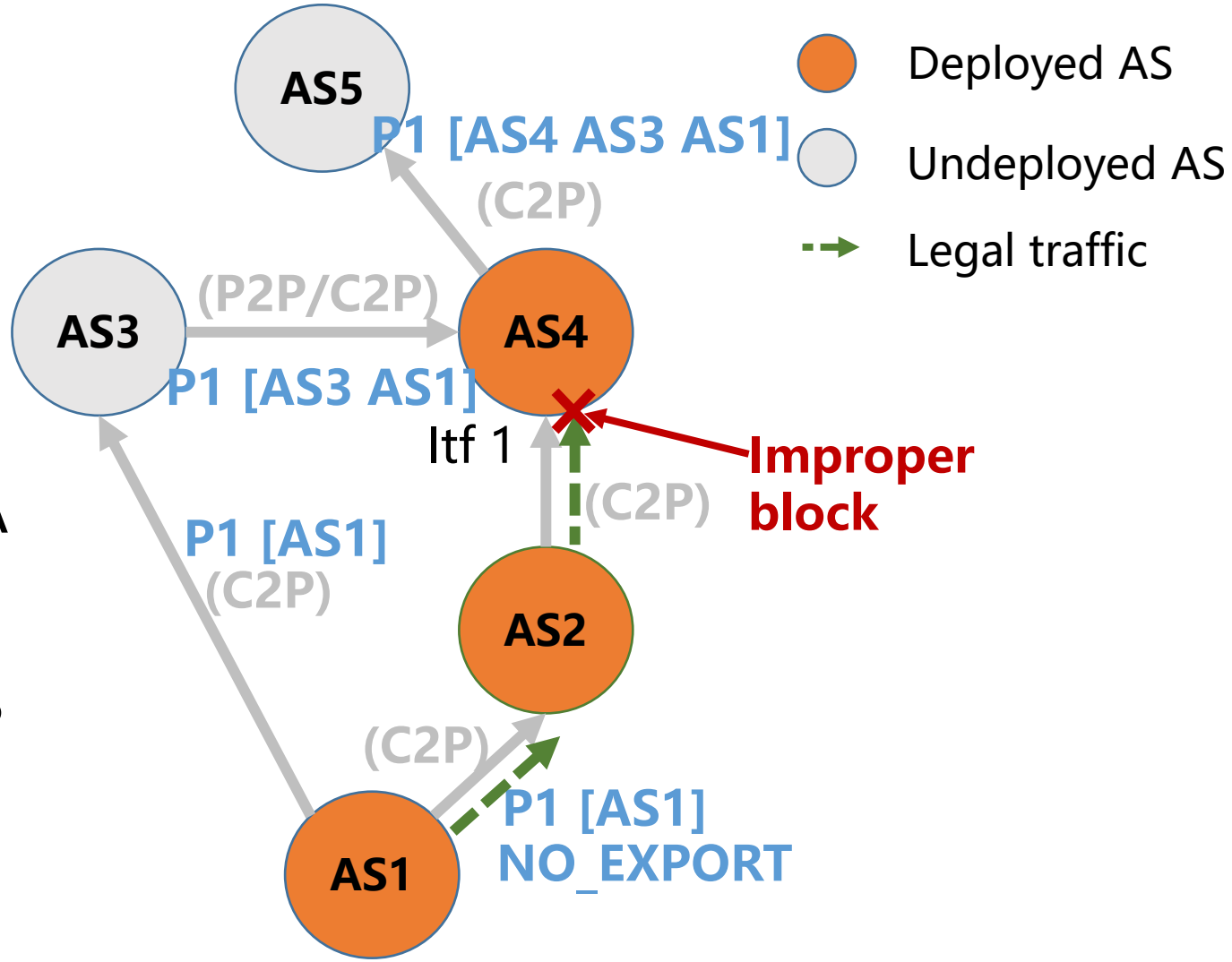
Gap #2: Improper Block

Scenario 3: NO_EXPORT in BGP Advertisement

- Forwarding path from AS1 to AS4: AS1->AS2->AS4

Behavior

- If AS4 runs EFP-uRPF Algorithm A
  - **Improper block** at Itf 1
- If AS4 runs EFP-uRPF Algorithm B
  - If AS3 is customer of AS4: no problem
  - If AS3 is peer of AS4: **improper block** at Itf 1



Scenario 3: NO_EXPORT in BGP Advertisement

Gap #2: Improper Block

- **Scenario 4: Anycast/Edge Hybrid--Direct Server Return (DSR)**
  - Request path: AS1->AS4->AS5
  - Tunnel path: AS5->AS4->AS2
  - Response path: AS2->AS4->AS1

Behavior

- If AS4 runs EFP-uRPF Algorithm A
  - **Improper block** at Itf 1
- If AS4 runs EFP-uRPF Algorithm B
  - **Improper block** at Itf 1