SAVNET's Incentive Consideration for Defense Against Reflection Attacks

Lancheng Qin, Dan Li, Jianping Wu, Li Chen, Fang Gao

Nov 11, 2022

Outline

- The Importance of Direct Incentive for SAV Deployment
- The Demand for Defense Against Reflection Attacks
- Incentive Comparison between EFP-uRPF and SAVNET
- Summary

The Importance of Direct Incentive for SAV Deployment

- Some ASes do not deploy BCP38 due to the misaligned incentive
  - "only prevents a provider who deploys SAV from originating spoofed-source traffic but does not protect the provider from receiving spoofed traffic or being the victim of an attack" [1]
  - "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" [2]
- To improve the adoption of SAV, SAV must provide direct incentive
  - If a network deploys SAV but finds that it only helps other networks, the network will not be motivated to deploy SAV
  - If a network deploys SAV and finds that sometimes it can help itself (compared with not deploying), the network will be more motivated to deploy SAV

Reference:
[1] Network Hygiene, Incentives, and Regulation: Deployment of Source Address Validation in the Internet. SIGSAC 2019
[2] Deployment of Source Address Validation by Network Operators: A Randomized Control Trial. S&P 2022

Outline

- The Importance of Direct Incentive for SAV Deployment
- The Demand for Defense Against Reflection Attacks
- Incentive Comparison between EFP-uRPF and SAVNET
- Summary

The Demand for Defense Against Reflection Attack

- Source address spoofing is mainly used in reflection attacks
  - An attacker forges the victim's IP address in requests sent to reflector
  - Preventing reflection attacks depends on the SAV filtering on path between the attacker and the reflector
- The market demand from customer or user networks
  - Customer or user networks ask their upstream providers to deploy SAV as close to the source as possible and to protect their source addresses from being forged
  - Network operators can improve their competitiveness by providing defense against reflection attacks

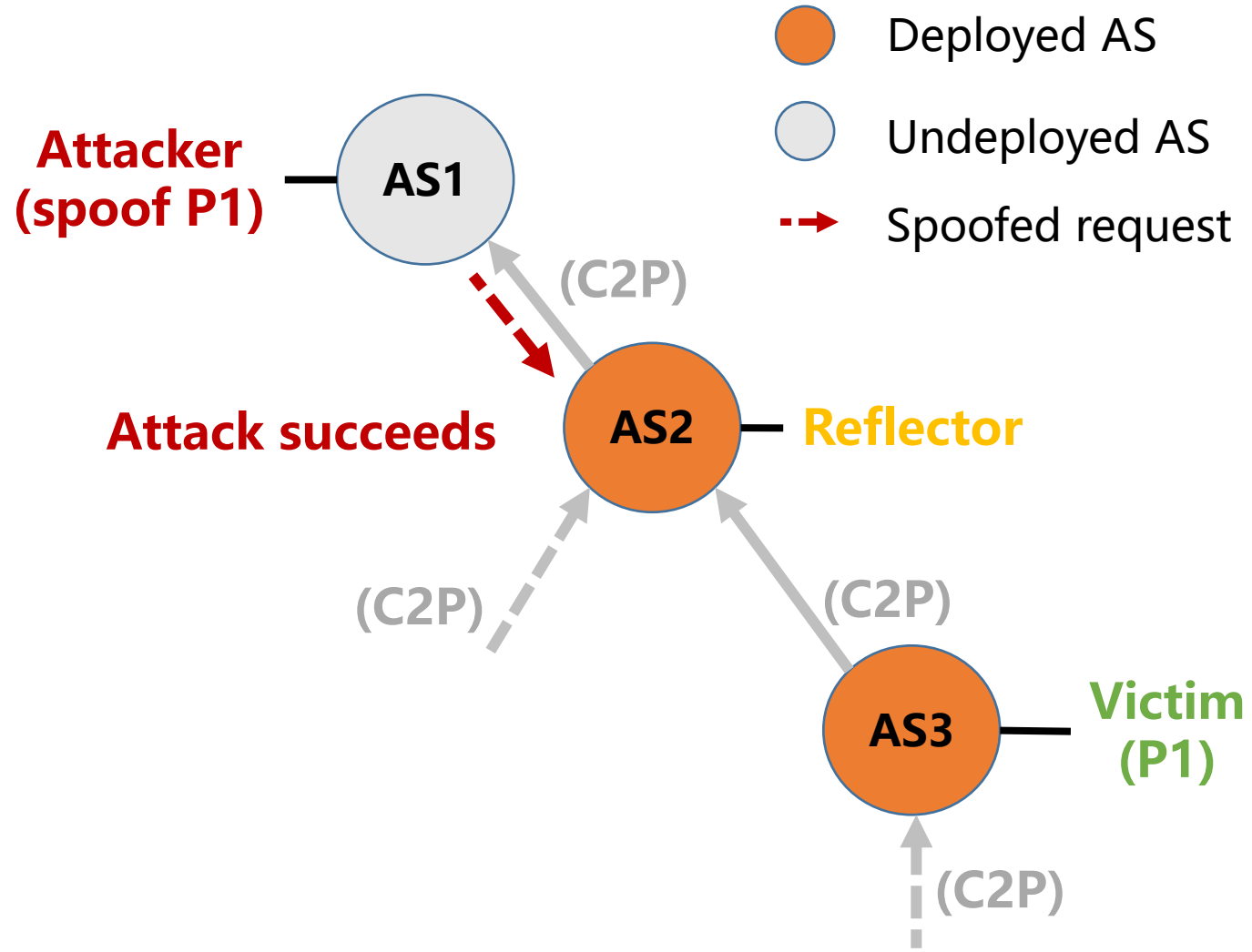
EFP-uRPF is not Well-aligned with the Demand

- EFP-uRPF is essentially deploying BCP38 at the top of a customer cone
  - It only validates traffic from customer interfaces but does not validate traffic from provider and peer interfaces
    - only prevents customer cone from originating spoofed traffic
    - does not protect the customer cone from receiving spoofed traffic or being the victim of a reflection attack from outside customer cone
  - EFP-uRPF algorithm B even compromises directionality among customer interfaces
- Network still suffers reflection attack even when it and its upstream providers have deployed EFP-uRPF

EFP-uRPF Fails to Prevent Reflection Attack

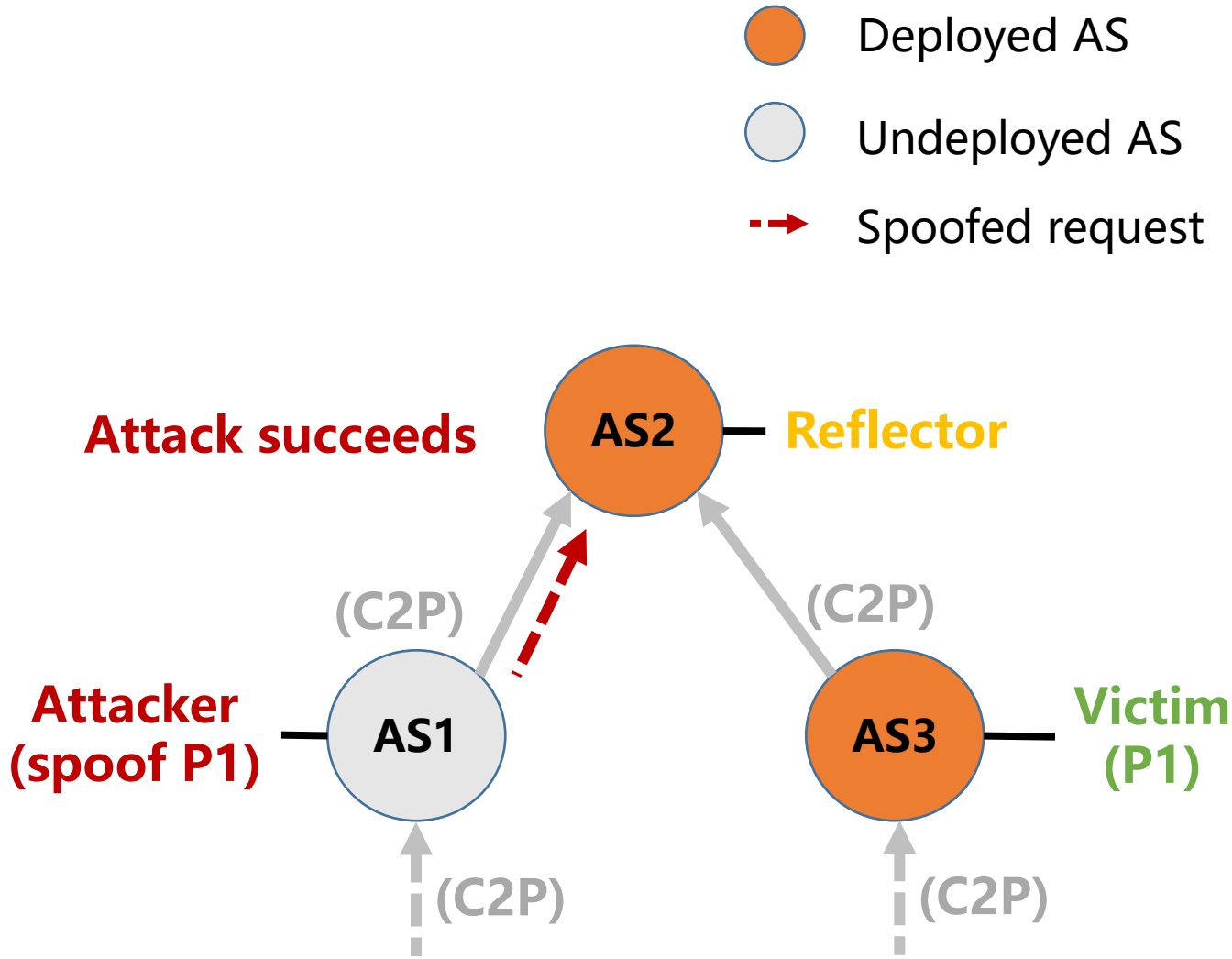
- Reflection attack
  - Attacker: AS1
  - Reflector: AS2
  - Victim: AS3

- Both EFP-uRPF algorithm A and EFP-uRPF algorithm B **fail**
  - Only working at customer interfaces
  - Lacking source address validation at provider and peer interfaces



EFP-uRPF Fails to Prevent Reflection Attack

- Reflection attack
  - Attacker: AS1
  - Reflector: AS2
  - Victim: AS3
- EFP-uRPF algorithm A works
- EFP-uRPF algorithm B **fails**
  - Compromising directionality among customer interfaces



Benefit of SAVNET Compared with EFP-uRPF

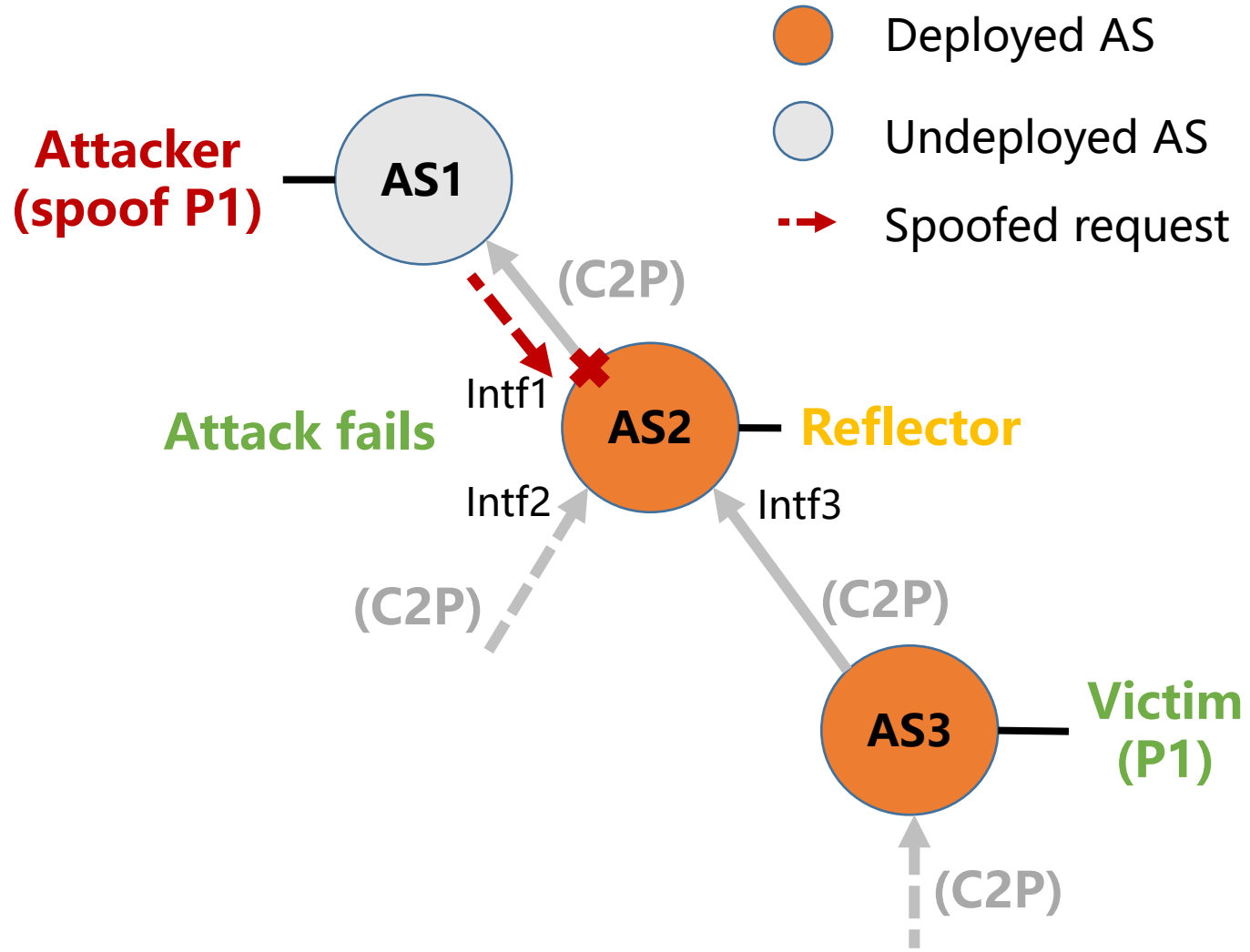
- Since there is no specific "SAVNET[1]" solution yet, we assume SAVNET could meet the following requirements:
  - ◆Validate traffic from all directions
  - ◆Match the real data-plane forwarding path originated from each deployed AS
- In this way, SAVNET would work better than EFP-uRPF at defending against reflection attacks

[1]: For the sake of description, we temporarily name a possible new SAV solution "SAVNET"

Benefit of SAVNET Compared with EFP-uRPF

- Reflection attack
  - ◆Attacker: AS1
  - ◆Reflector: AS2
  - ◆Victim: AS3

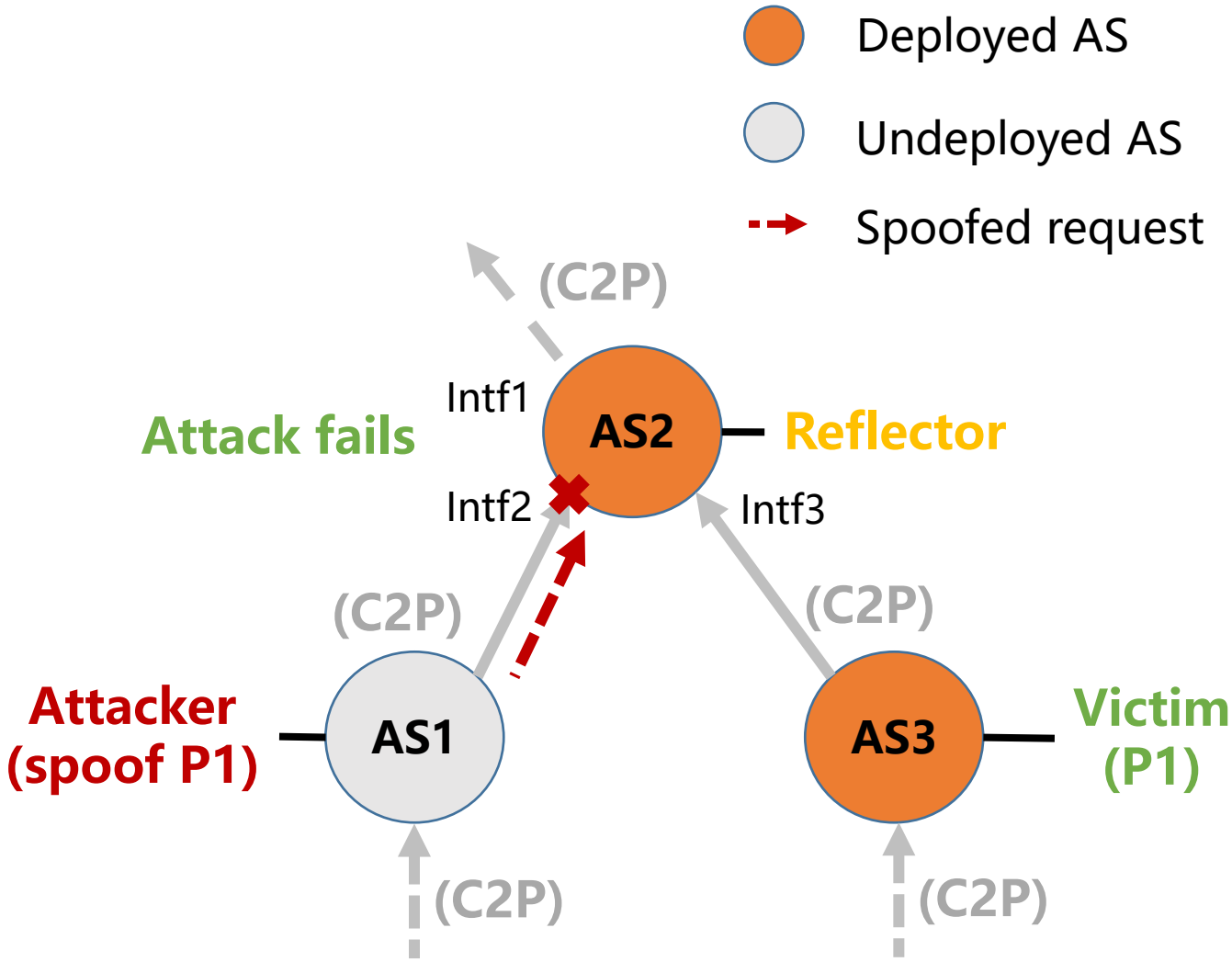
- SAVNET **works**
  - ◆SAVNET notifies AS2 of the real incoming interface (i.e., Intf 3) for source addresses of AS3 (i.e., P1)
  - ◆AS2 rejects the request with spoofed source addresses of P1 from other incoming interfaces (e.g., Intf1)



Benefit of SAVNET Compared with EFP-uRPF

- Reflection attack
  - ◆Attacker: AS1
  - ◆Reflector: AS2
  - ◆Victim: AS3

- SAVNET **works**
  - ◆SAVNET notifies AS2 of the real incoming interface (i.e., Intf 3) for source addresses of AS3 (i.e., P1)
  - ◆AS2 rejects the request with spoofed source addresses of P1 from other incoming interfaces (e.g., Intf2)



Outline

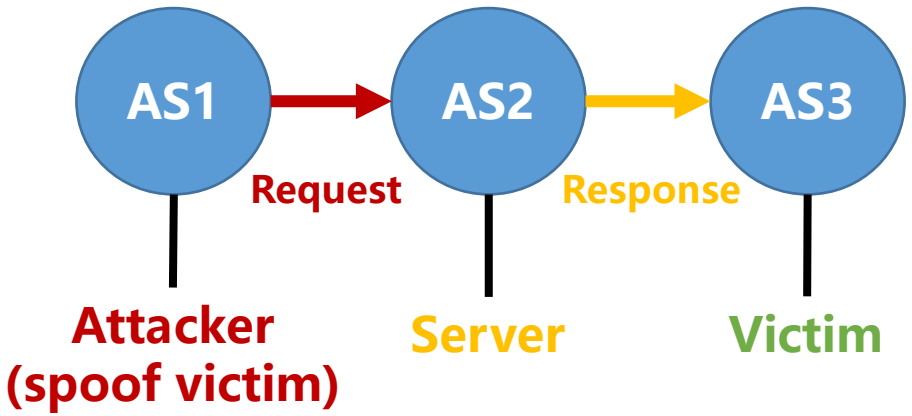
- The Importance of Incentive for SAV Deployment
- The Demand for Defense Against Reflection Attacks
- Incentive Comparison between EFP-uRPF and SAVNET
- Summary

Comparison Methodology

- Using reflection attack as the case
  - ◆Roles: attacker, reflector, victim
- Comparison
  - ◆Assume the victim network always deploy SAV mechanism (EFP-uRPF or SAVNET), because only the victim network benefits from the defense against reflection attacks
  - ◆For any deploying cases of the other two networks (attacker, reflector)
    - ➢Check whether the reflection attack can be prevented
    - ➢If so, the victim can be motivated to deploy SAV
    - ➢If not, the victim cannot benefit from deploying SAV

Results in Scenario #1

Scenario #1

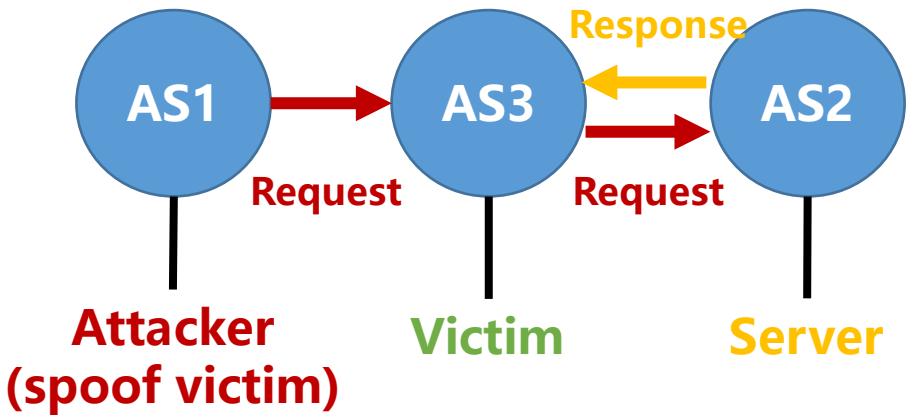


- SAVNET works in **75%** cases
- EFP-uRPF algorithm A works in **30%** cases
- EFP-uRPF algorithm B works in **20%** cases

SAV deployment	AS1 to AS2	AS2 to AS3	EFP-uRPF A	EFP-uRPF B	SAVNET
AS3 deploys SAV	P2C	P2C	Fail	Fail	Fail
	P2P	P2C	Fail	Fail	Fail
	C2P	C2P	Fail	Fail	Fail
	C2P	P2P	Fail	Fail	Fail
	C2P	P2C	Fail	Fail	Fail
AS3 and AS1 deploys SAV	P2C	P2C	Fail	Fail	Work
	P2P	P2C	Fail	Fail	Work
	C2P	C2P	Fail	Fail	Work
	C2P	P2P	Fail	Fail	Work
	C2P	P2C	Fail	Fail	Work
AS3 and AS2 deploy SAV	P2C	P2C	Fail	Fail	Work
	P2P	P2C	Fail	Fail	Work
	C2P	C2P	Work	Work	Work
	C2P	P2P	Work	Work	Work
	C2P	P2C	Work	Fail	Work
AS3, AS2, and AS1 deploy SAV	P2C	P2C	Fail	Fail	Work
	P2P	P2C	Fail	Fail	Work
	C2P	C2P	Work	Work	Work
	C2P	P2P	Work	Work	Work
	C2P	P2C	Work	Fail	Work

Results in Scenario #2

Scenario #2

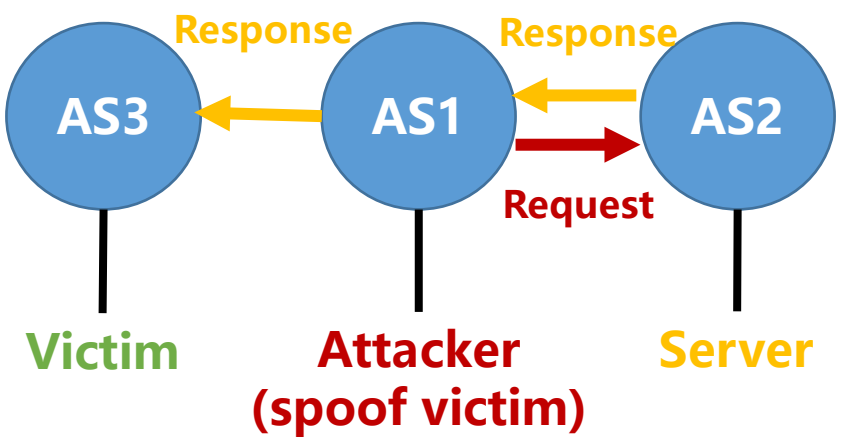


- SAVNET works in **100%** cases
- EFP-uRPF algorithm A works in **60%** cases
- EFP-uRPF algorithm B works in **60%** cases

SAV deployment	AS1 to AS2	AS2 to AS3	EFP-uRPF A	EFP-uRPF B	SAVNET
AS3 deploys SAV	P2C	P2C	Fail	Fail	Work
	P2P	P2C	Fail	Fail	Work
	C2P	C2P	Work	Work	Work
	C2P	P2P	Work	Work	Work
	C2P	P2C	Work	Work	Work
AS3 and AS1 deploys SAV	P2C	P2C	Fail	Fail	Work
	P2P	P2C	Fail	Fail	Work
	C2P	C2P	Work	Work	Work
	C2P	P2P	Work	Work	Work
	C2P	P2C	Work	Work	Work
AS3 and AS2 deploy SAV	P2C	P2C	Fail	Fail	Work
	P2P	P2C	Fail	Fail	Work
	C2P	C2P	Work	Work	Work
	C2P	P2P	Work	Work	Work
	C2P	P2C	Work	Work	Work
AS3, AS2, and AS1 deploy SAV	P2C	P2C	Fail	Fail	Work
	P2P	P2C	Fail	Fail	Work
	C2P	C2P	Work	Work	Work
	C2P	P2P	Work	Work	Work
	C2P	P2C	Work	Work	Work

Results in Scenario #3

Scenario #3



- SAVNET fails
- EFP-uRPF algorithm A fails
- EFP-uRPF algorithm B fails

SAV fails when victim's source address shares the same incoming interface with the attacker's source address in the SAV rule

SAV deployment	AS1 to AS2	AS2 to AS3	EFP-uRPF A	EFP-uRPF B	SAVNET
AS3 deploys SAV	P2C	P2C	Fail	Fail	Fail
	P2P	P2C	Fail	Fail	Fail
	C2P	C2P	Fail	Fail	Fail
	C2P	P2P	Fail	Fail	Fail
	C2P	P2C	Fail	Fail	Fail
AS3 and AS1 deploys SAV	P2C	P2C	Fail	Fail	Fail
	P2P	P2C	Fail	Fail	Fail
	C2P	C2P	Fail	Fail	Fail
	C2P	P2P	Fail	Fail	Fail
	C2P	P2C	Fail	Fail	Fail
AS3 and AS2 deploy SAV	P2C	P2C	Fail	Fail	Fail
	P2P	P2C	Fail	Fail	Fail
	C2P	C2P	Fail	Fail	Fail
	C2P	P2P	Fail	Fail	Fail
	C2P	P2C	Fail	Fail	Fail
AS3, AS2, and AS1 deploy SAV	P2C	P2C	Fail	Fail	Fail
	P2P	P2C	Fail	Fail	Fail
	C2P	C2P	Fail	Fail	Fail
	C2P	P2P	Fail	Fail	Fail
	C2P	P2C	Fail	Fail	Fail

Outline

- The Importance of Incentive for SAV Deployment
- The Demand for Defense Against Reflection Attacks
- Incentive Comparison between EFP-uRPF and SAVNET
- Summary

Summary

- For any attack scenario or deployment case, we find that SAVNET could work better or not worse than EFP-uRPF

- Therefore, a network could have more incentive to deploy SAVNET as the SAV mechanism, because it would have high probability of defending against reflection attacks