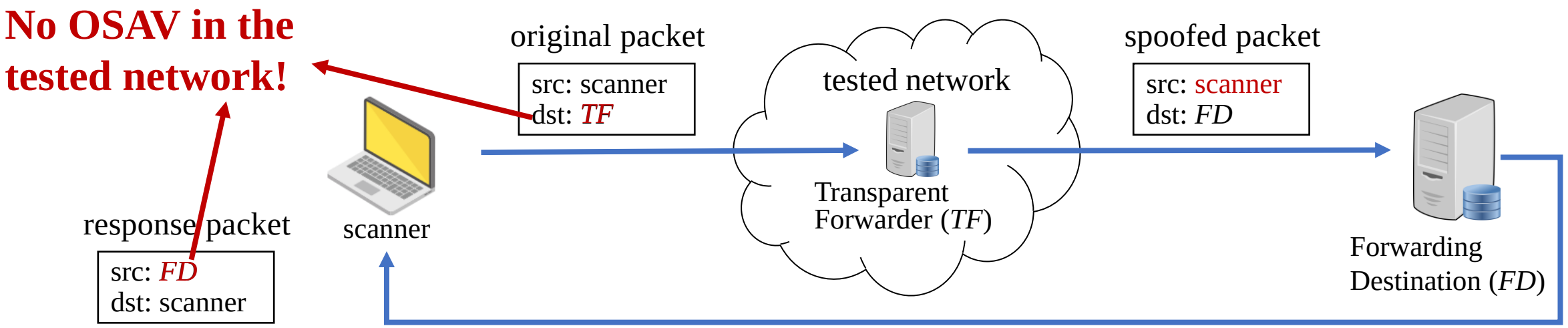
IETF 120

Identifying the Presence of Outbound Source Address Validation (OSAV) Remotely

Shuai Wang
Zhongguancun Laboratory

July 24, 2024

How to identify the absence of OSAV remotely?



(1) Find a Transparent Forwarder (*TF*) in the tested network

(2) Send a packet from the scanner to the *TF*

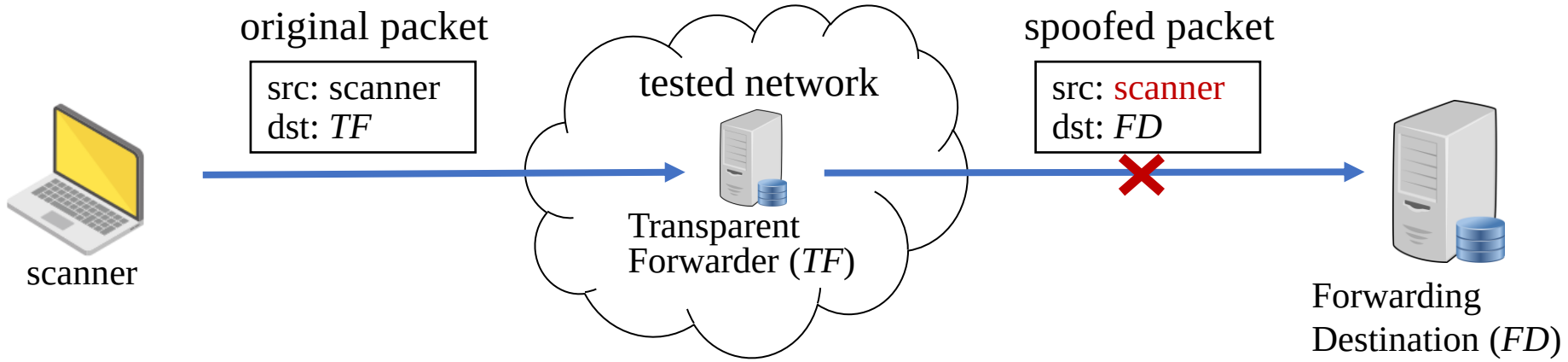
(3) The *TF* forwards the packet, with scanner as source IP and *FD* as destination IP, i.e., a spoofed packet

(4) The *FD* receives the spoofed packet and directly respond to the scanner

We can learn that the spoofed packet is not discarded (i.e., no OSAV) by comparing the query and the response.

[1] M Kührer, et al., Exit from hell? Reducing the impact of amplification DDoS attacks. USENIX Security'14

What will happen if OSAV is deployed?



The spoofed packet is discarded by OSAV. → The FD cannot receive the spoofed packet. → The scanner will not receive any response.

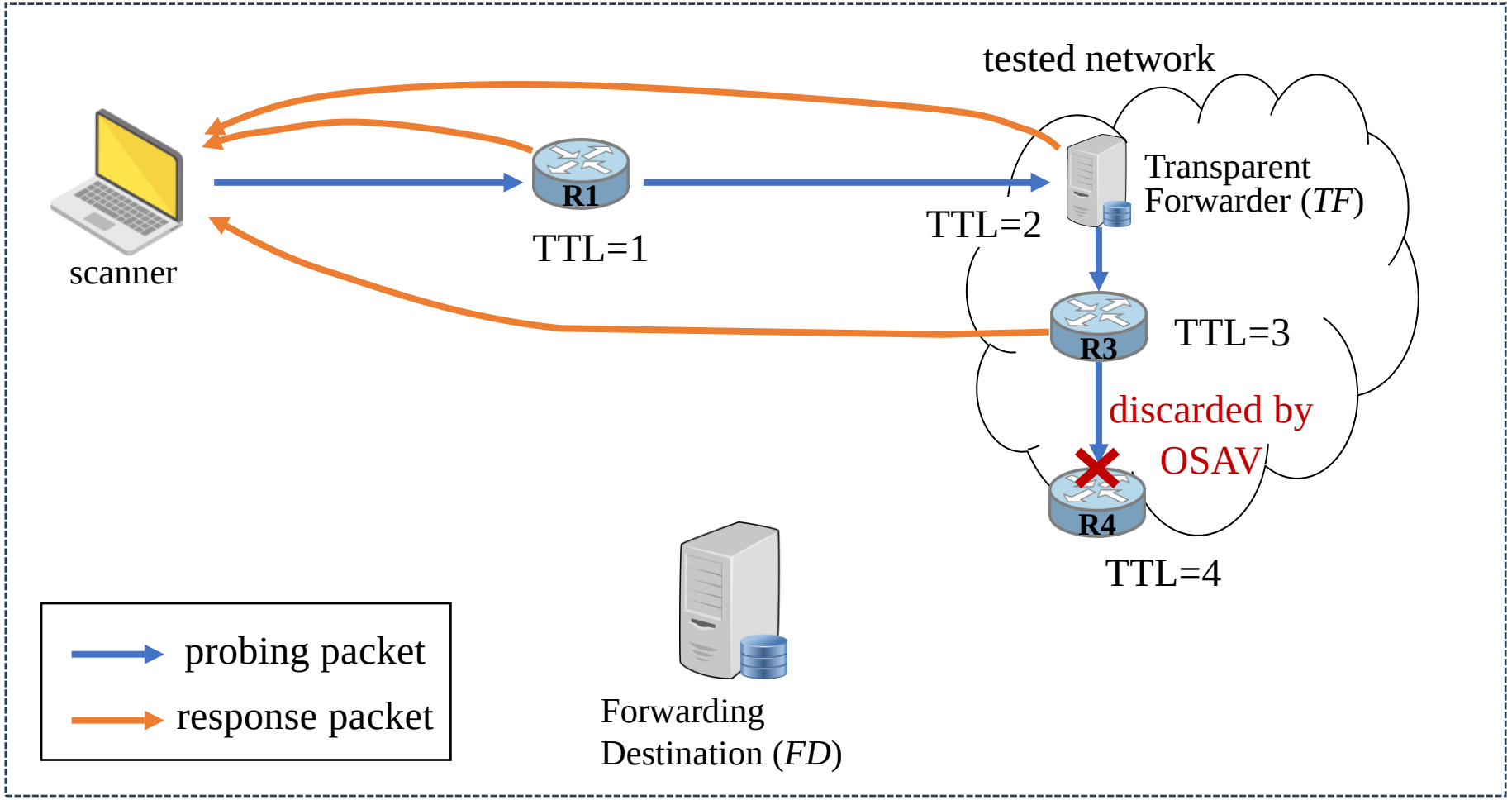
☹ **We do not know in advance which IP address is used by a transparent forwarder**

The original packet is not sent to a TF. → The FD cannot receive the spoofed packet. → The scanner will not receive any response.

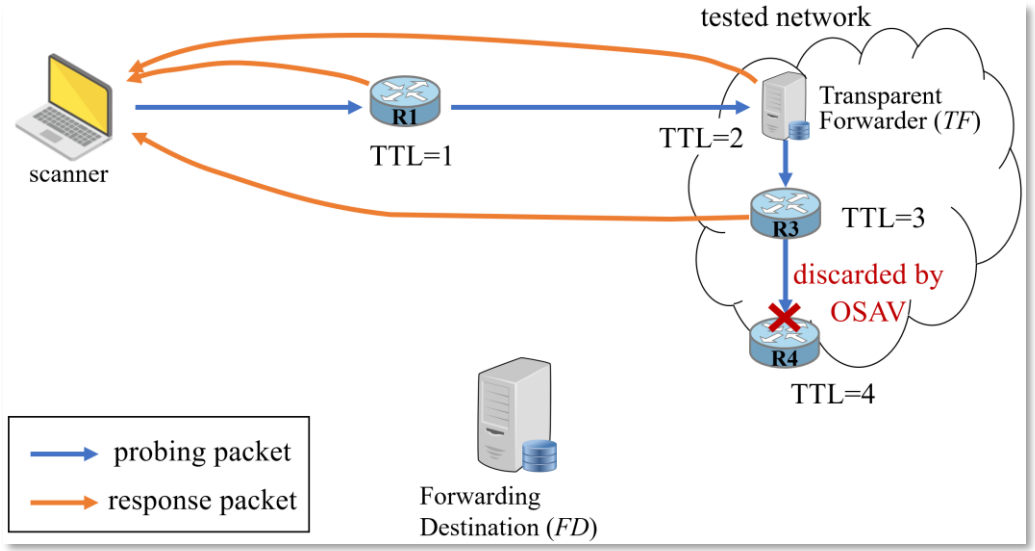
OSAVRoute can distinguish them

Based on traceroute, OSAVRoute can track the path of a data packet and know whether a spoofed packet is generated

Hop	Node in the path
1	R1
2	TF (tested IP)
3	R3



OSAVRoute can distinguish them




```
Internet Protocol Version 4, Src: 142.251.70.105  Dst: [redacted]169
Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0xc772 [correct]
    [Checksum Status: Good]
    Unused: 00
    Length: 17
    [Length of original datagram: 68]
    Unused: 0000
    Internet Protocol Version 4, Src: [redacted].169, Dst: 8.8.8.8
    User Datagram Protocol, Src Port: 38859, Dst Port: 33448
```

Node in the path

Destination of probing packet

ICMP response packet

Hop	Node in the path	Destination of probing packet
1	R1	TF
2	TF (tested IP)	TF
3	R3	FD

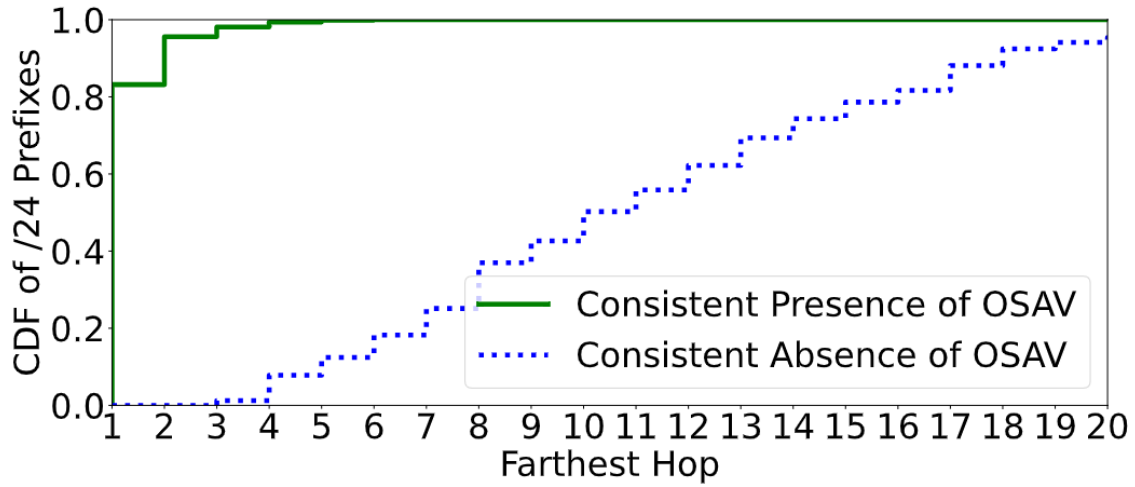
A spoofed packet is generated !

Transparent forwarder

- We discovered 2.25M transparent forwarders by sending DNS queries and TCP SYN packets to every single routable IPv4 address
- After removing transparent forwarders that cannot help us infer OSAV deployment, 6.61K transparent forwarders fail to send spoofed packets outside their origin ASes
  - ✓ The forwarding destination is in the same AS as the transparent forwarder
  - ✓ The transparent forwarder *may* be a router in transit Ases
  - ✓ The IP address of transparent forwarder is unknown
  - ✓ The transparent forwarder *may* be multi-homed
  - ✓ (There may be more cases that need to be removed due to the complicated Internet)

Measurement results

- Our measurement results show that 440 ASes deployed OSAV, where 169 ASes are identified by sending TCP SYN packets
  - ✓ One prefix is also measured by CAIDA Spoofer, confirming the presence of OSAV, which aligns with OSAVRoute
  - ✓ 83% of spoofed packets reaches their farthest hop at the first hop, and only 1.9% of spoofed packets are transmitted beyond three hops
    - ➢ This distribution is similar to prior work based on CAIDA Spoofer



Protocol	# of Prefixes	# of ASes
DNS	781	271
TCP/21	43	42
TCP/53	240	138
TCP/80	90	58
TCP/443	240	98
TCP/4567	53	48
TCP/7547	47	45
TCP/8080	83	55
All	1,228	440

Responsible disclosure

- The measurement results are published on our website https://ki3.org.cn/#/sav and updated monthly
  - ✓ including spoofable prefixes, blocked prefixes, and inconsistent prefixes
- We are working to contact network operators to inform them of the SAV deployment in their networks
  - ✓ A large ISP in China has acknowledged our measurement results for some of their prefixes

Next Step

- **Results Validation:** We encourage researchers and network operators to independently validate our measurement results and provide feedback. We will also report our results to the corresponding network operators
  - ✓ including both **presence of OSAV** and **absence of OSAV**
- **Community Collaboration:** We invite the community to participate in OSAVRoute measurement. Based on the feedback, we will continue to refine OSAVRoute

If you are interested in collaborating or have suggestions on how we can enhance our measurement framework, please reach out to us!

Thanks!

wangshuai@zgclab.edu.cn