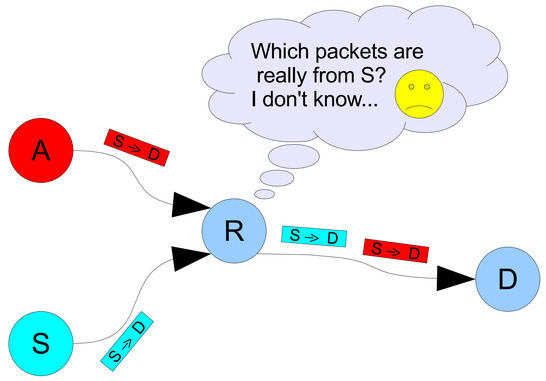
ID³: An **I**ncrementally **D**eployable **I**ncoming **D**irection **ID**entification Protocol

Toby Ehrenkranz <tehrenkr@cs> Advisor : Jun Li <lijun@cs>

Problem

- Routers cannot know the valid incoming direction of packets from a given source address.
- Routers simply forward packets to the destination without validating the source address.
- Attackers hide their identities

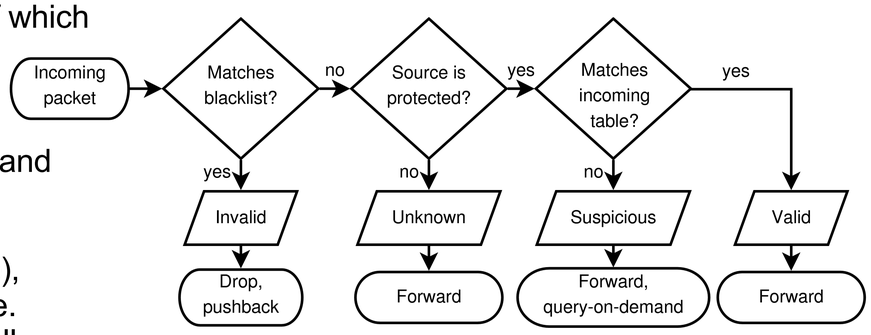


But what about ... ?

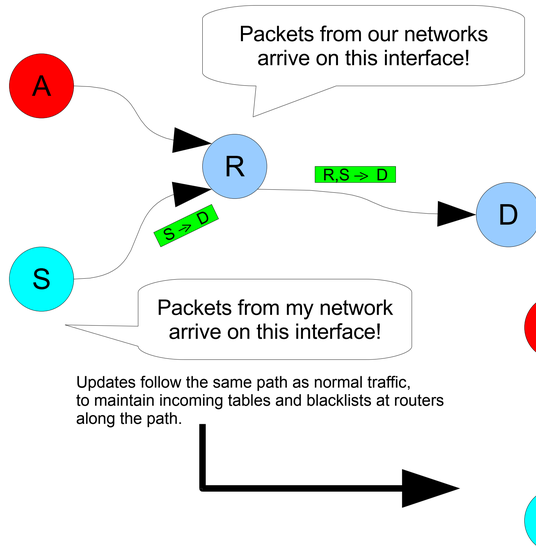
- Ingress/Egress filtering is not enough! Not effective without nearly full deployment.
- Asymmetric routing is common – you cannot assume the route to an address is the same as the route from an address.
- Newer proposed solutions have poor performance, or assume specific routing policies or protocols.
- Botnets can attack without spoofing traffic, but botnet owners still want to spoof in order to keep the botnet “zombies” anonymous.
- MIT Spoofer project estimates end-hosts can spoof more than 18% of all Internet addresses (and that is only counting hosts behind routers that do perform at least some ingress filtering!!!)

The ID³ Solution

- Use incoming table to keep track of which interface a packet with some source should arrive on.
- Use blacklist to keep track of which interface a packet with some source and destination should not arrive on.
- When unsure of incoming interface information (maybe a routing change), query the source router for an update.
- When classifying invalid packets, tell upstream routers to also drop similar invalid packets.

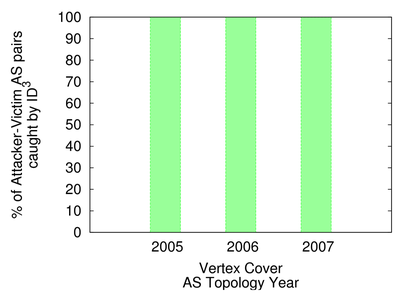


Contact the author for further details on incremental deployment problems and solutions, and how we secure the protocol against attackers.

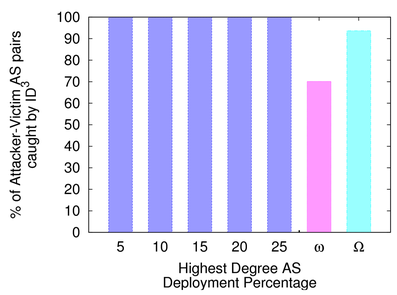


Efficacy

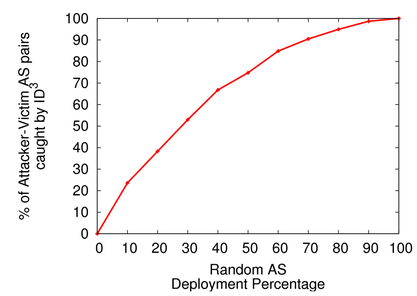
- Measure the percentage of attacker-victim AS pairs where the attacker cannot successfully spoof a protected source to that victim AS.
- Use Internet AS topologies generated from BGP data collected by the Route Views project.
- Consider a variety of types of deployment locations, from a vertex cover (best case) to random deployment (worst case).



If deployed as a vertex cover the efficacy is nearly perfect, but such a deployment is difficult to achieve. Each year a vertex cover required about 15% of the ASes.



Deployment at only the highest degree ASes is also not likely, but deploying at some subset of higher degree ASes should be achievable and is effective.
ω : purely random selection of half of the top 30% of ASes (by degree)
Ω : weighted random selection of half of the top 30% of ASes (by degree)
(weighted such that the probability of selection is proportional to the AS degree)



Random deployment would not be effective. Deployment should be planned at least a little to target the higher degree Ases first.