ID³: An Incrementally Deployable Incoming Direction IDentification 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.

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.

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).