Prefix hijacking

- Anyone can advertise routes for any prefix!
- How can hijacker get the advertised routes to actually be used by other ASes?
  1. Announce more specific (longer) prefix than real owner
  2. Now everyone’s traffic is “blackholed”
- Can protect against this (Secure BGP) but it’s not deployed in today’s Internet
From hijacking to Man In The Middle

- August '08, Kapela and Pilosov
- Traffic to a destination redirected (not blackholed) through an attacker
- Attacker can watch everything you do without you noticing
- What's the key problem here?

How can attacker forward traffic to destination, if attacker is pretending to be the destination?

Hijacking + eavesdropping

1. A finds legitimate announcement for path ABD to 128.2.0.0/16

BGP Announcements
1. A finds legitimate announcement for path ABD to 128.2.0.0/16

2. A sends bogus announcement for path ABD to 128.2.0.0/24

3. Result: ASes (here B) on real path keep using real path (loop elimination)

4. All other ASes use route through A

5. A forwards traffic to B

Kapela & Pilosov also described how to spoof traceroute information to be even more undetectable.