# Multi6 Threats

draft-nordmark-multi6-threats-00.txt

Design Team Members (alphabetical order):
Iljitsch van Beijnum, Steve Bellovin, Brian Carpenter, Mike O'Dell, Sean Doran, Dave Katz, Tony Li, Erik Nordmark, and Pekka Savola

# Why?

- Allowing locators to change opens up potential security holes
  - Loosely called “redirection attacks”
  - Also potential concerns about accepting packets
- These attacks can be used to
  - Divert traffic
  - Denial of Service of a 3rd party
- Similar, but not identical, threats to Mobile IPv6
  - Need to write down the multihoming threats

# Application Assuumptions Today

- Initiator might use DNS and, if so, trust the returned IP address(es)
- Responders:
  - Public content servers – doesn't care who is asking
  - Trust source IP address without any verification (very bad!)
  - Trust source IP address after reverse+forward DNS lookup (bad!)
  - Security (IPsec, TLS, etc) using its notion of identity
  - Opportunistic security without access control

# Redirection Threats Today

- Routing can be compromised
- DNS can be compromised
- ND/ARP spoofing on one link along the path
- Attack on node (endpoint, router, switch) or wire along the path
- Top 3 are the subject of work in the IETF
- A multihoming solution shouldn't make things worse

# Some flooding attacks today

- Send packets towards target
  - Limited my attackers access link bandwidth
- Flood myself or path towards myself
  - Send TCP acks for packets not received - sender pumps data towards me even if path is congested
  - Attacker could claim to be other node on the path
- Reflection attacks
  - If X can send packet to B to causing B to send packets to A; with or without amplification
  - Combined with source address spoofing

# Potential New Attacks; packets to attacker

- Redirect an existing flow to a new locator
  - Might require only a single packet and be persistent
- Premeditated redirection
  - X predicts A will talk to B
  - X communicates with B claiming to be A and presents its locators
  - When A arrives it might look like an attacker to B
- Replays
  - If A was previously at a locator, can attacker replay message from A causing packets to go to old place?

# Potential New Attacks; black hole

- Attacker could cause packets to be sent to nonexistent/unreachable locator
  - Selectively DoS some communication
- Note that in the precense of secured content (IPsec, TSL, etc) attacks on previous slide all are limited to black holing

# Potential New Attacks; 3rd party DoS

- Attacker with limited link bandwidth using redirection to flood 3rd party
  - X initiates communication with B which has lots of bandwith
  - X later tells B that is it reachable at A's locator causing B to switch
  - X can probably sustain the flood of A by injecting “ACK” packets to B
- Check that the node is indeed reachable at locator
  - But is it sufficient for X to be on A's path for a short time?

# Accepting Packets?

- Today where ingress filtering is used
- Hard for off-path attacker to inject a packet in some packet flow
  - The ULP is identified by the source IP address
- With multihoming receiver potentially accepts packets with any source locator
  - Would make ingress filtering ineffective
- Could limit to verified locators, or have other technique to prevent off-path attackers
  - Such as SCTP verification tag concept

# Other security concerns

- Avoid having any new protocol mechanism have security problems of their own
  - Don't create state on the first packet in an exchange
  - Don't do much work on the first packet
- Potential chicken-and-egg issue
  - Don't want to create state/do work until peer id/loc verified
  - But need state/work to do that verification
- Defering state/work somehow

# Open Issues

- Mail from Pekka