

draft-nordmark-multi6-threats

Erik Nordmark
Tony Li

Changes since -00

- Added reference to [DNS-THREATS] and clarified that attackers on the path between the host and the DNS servers can redirect traffic today.
- Added a section on existing packet injection attacks to talk about TCP sequence number guessing etc.
 - Need to add RST example to text
- Clarified ingress filtering relationship in section on today's flooding attacks
- Added section on privacy
 - Need to add something about current level of privacy

Work in progress

- Added a new section on granularity to list some issues about transport-level versus IP-level approaches and what we understand about the differences in security
- Added a new section on movement to discuss how things change when hosts move around the network
- Added Appendix B with some security arch analysis
 - Should probably be moved to a different document to keep this document focused on the threats

Potential Open Issues

- Does this apply to schemes without a new ID name space?
 - I think so; even with id being a FQDN or a list of locators the same threats are present
- Granularity in space and time?
 - Part of threats or part of security analysis?

Document Outline (1)

- Assumptions
 - “Do no harm” - current IPv4 Internet
- Today
 - Applications use of IP addresses today
 - Redirection attacks today
 - Packet injection today
 - Flooding today
 - (Missing) address privacy today

Document Outline (2)

- Potential new redirection attacks
 - Redirection to the attackers
 - Once packets are flowing
 - Premeditated redirection
 - Replays
 - Redirection to a black hole
 - Third party Denial-of-Service
 - Accepting packets from unknown locators
- Other security concerns
 - E.g., make sure new protocol is secure itself

