TCP SYN Flooding Attacks and Common Mitigations

Wesley M. Eddy
Verizon / NASA
weddy @ grc.nasa.gov

Background

- Attack well known/understood
  - Mitigation techniques commonly implemented
- During TCP Roadmap work, this was felt to be something important to document
  - Several advisories, academic papers, etc. are available
  - But no guidance from IETF or RFC series

Status

- Accepted as WG item
  - Current version is draft-eddy-syn-flood-02
  - WG version available soon
- Goals:
  - Clear technical description of attack
  - Overview of mitigations, their implications, and advice for both implementers and network/server administrators

What's Needed?

- More WG input
  - Especially from implementors
    - Have heard from some commercial vendors and some open-source projects
    - Want to hear more, including strategies and rationale that have been used
  - Are there any real-world success stories for particular mitigations?
  - Notes on specific applications (e.g. SMTP)