draft-tcpm-tcp-antispoof

Joe Touch

Postel Center Director

Research Assoc. Prof. CS & EE

USC/ISI

Changes from draft-touch-tcp-antispoof

- ←Remove derivative works statement
- ←Refer to attacks properly
  - ←Analysis of potential attacks, not seen *in the wild* yet (?)
- ←Omit BTNS work (3 pages)
  - ←Summarized and cited that I-D instead
- ←Address focus throughout (5 pages)
  - ←Left objective (IMO) facts comparing alternatives
  - ←Removed positions on preferred solution

Additional mods pending

- ← Update references
  - ← Initial observation: Convery, Sean and Franz, Matthew; "BGP Vulnerability Testing: Separating Fact from FUD", 2003, http://www.nanog.org/mtg-0306/pdf/franz.pdf
    - ← *assumes attack must cover entire seq space, not just 'in window'*
  - ← Analysis of attack: Watson, P., "Slipping in the Window: TCP Reset attacks," Presentation at 2004 CanSecWest. http://www.cansecwest.com/archives.html
    - ← *fails to note N^2 factor impact of BW increase*
    - ← *does not discuss/categorize variety of current solutions*
- ← Updated discussion of RFC793 rules
  - ← *For RSTs, seq num may be checked, but should thus be discarded* (not ACK'd ☺) … effect of discard on rebooting systems not considered
- ← Cleanup refs to windowing
  - ← Receive window issues per se, incl. data pickup by app.
- ← Long list of typos…
  - ← (thanks, Pekka)

Receive Window issues

- NOT congestion window
- Receive window related:
  - **RCV.NXT ≤ SEG.SEQ < RCV.NXT+RCV.WND**
  - **RCV.NXT ≤ SEG.SEQ+SEG.LEN-1 < RCV.NXT+RCV.WND**
- *Indirectly* depends on BW*delay
  - "SHOULD" be at least BW*delay (documented?)
  - "SHOULD" be larger (handle periodicity of application drain)
- May be zero (e.g., if app. leaves data in socket)
  - "special allowance should be made to accept valid ACKs, URGs and RSTs. [in that case]" – RFC793
  - What is valid in that case, esp. if above checks are in place?

Other requested mods

- Address "other solutions" (seem flawed)
  - Ingress filtering
    - Not local to endpoint pair
  - TTL checks
    - Used for BGP
    - *Partial* protection of secure tunnel
    - Vulnerable to anyone "1-hop" away (incl. tunnels)
- Address title
  - "spoofing" vs. "identity spoofing" (needed?)
- ICMP attacks as related?
  - Cite, but note as distinct
- BGP stability (drop TCP = drop routes)
  - find citation