draft-ietf-tcpm-tcpsecure-02.txt

IETF 62, Minneapolis
10th March 2005

Mitesh Dalal
(Editor)
Cisco Systems

Summary/Recap

- RST/SYN Attack:
  - RST acceptable only on an exact match of the sequence number. ACK challenge for anywhere else in the acceptable window.
  - For SYN, irrespective of its sequence number send an ACK.
- Data injection:
  - Check for ACK value to go back at most the max window advertised to peer.

Changes from -00 draft

- For the SYN attack, in the earlier draft, we proposed to subtract 1 from the SEG.ACK of challenge ACK for the condition

  (SEG.SEQ of SYN == RCV.NXT)

- New solution: Send an ACK with SEG.ACK of RCV.NXT, irrespective of the SEQ value of the incoming SYN.

Changes from -00 draft

- Implementations SHOULD
  - introduce port randomization
  - ACK throttling to stop ping pong of packets with non-compliant TCP implementations/ firewalls that cache RSTs.
- Scenario that might require more than 1 RTT to successfully terminate connection.
- Minor typos corrected.

…and finally

- Incorporates almost all the feedback received from the WG.
- Authors feel comfortable with the details in the document.
- Running in the field for over a year with zero reported issues.
- At least 7 vendors have implemented this draft.
- More questions / WGLC ?