Improving TCP robustness (A brief status report)

draft-ietf-tcpm-tcpsecure-07.txt

Anantha Ramaiah

Summary

- Provides mitigations to RST, SYN and Data injection.
- Thoroughly discussed in the TCPM list since its inception to take the current shape.
- Running in the Internet for about 2 years. Many vendors have implemented these mitigations.
- Version -07- submitted recently.

Recent changes (ver. 06 and 07)

- All mitigation recommendations changed from MUST to SHOULD.
- Security considerations section rewritten to address the comments.
- Other minor comments like add explicit reference to MD5, various editorial comments, typos, grammar errors etc.,

Data Injection – SHOULD or MAY

- A concern was raised in the mailing list about whether this mitigation be tagged a SHOULD or MAY.
- The data injection mitigation says, make sure the ACK value is in the range :-

  (SND.UNA - MAX.SND.WND) <= SEG.ACK <= SND.NXT

  Where MAX.SND.WND is the largest window advertised by the peer.
- Implementations can chose to hard code the value of MAX.SND.WND. For Eg:- 65535.
- This mitigation also increases the robustness for FIN attacks.

Questions

- More comments welcome ☺
- WGLC?

Thankyou!