DoS vulnerability of TCP by acknowledging not received segments

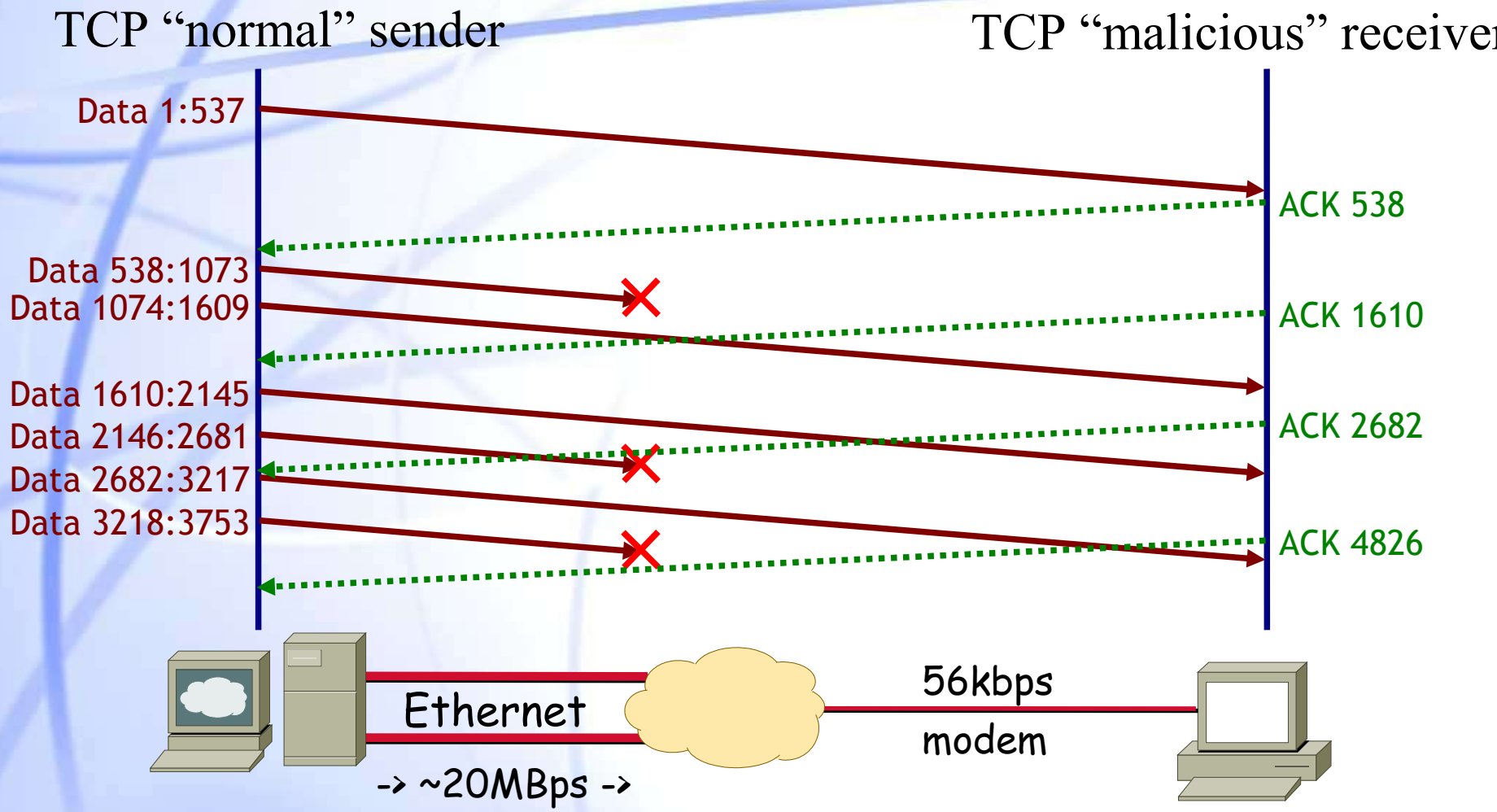
draft-azcorra-tcpm-tcp-blind-ack-dos-01

By
Arturo Azcorra <azcorra@it.uc3m.es>
Carlos J. Bernardos <cjbc@it.uc3m.es>
Ignacio Soto <isoto@it.uc3m.es>

Dept. Telematic Eng. – University Carlos III of Madrid
2004-08-02
60th IETF – San Diego

Departamento de INGENIERIA TELEMATICA
www.it.uc3m.es

Expeditious Blind ACK DoS



DoS attack to information servers!!

Proposed Solutions (I)

- These modifications could be used independently or together
- 1. Starting a slow start procedure
  - A server MUST start the slow start procedure if it receives an ACK for unsent data, but within the transmitter send window:
    - SND.NXT < SEG.ACK <= SND.UNA+SND.WND
  - Intended to penalize an attacker
  - This modification couldn't be used by a malicious THIRD party to attack a legitimate TCP connection

Proposed Solutions (II)

- 2. Matching SEG.ACK and (SEG.SEQ + SEG.LEN)
  - A server SHOULD randomize segment boundaries in the range [MS, a*MS]
    - MS = current maximum segment size
    - a = number in the range [0,1]
  - A server should accept an ACK, but NOT increase its CWND variable, if the SEG.ACK fulfils these 2 conditions simultaneously:
    - SND.UNA <= SEG.ACK <= SND.NXT
    - SEG.ACK <> (SEG.SEQ + SEG.LEN) of one of the unacknowledged segments that have been sent