CSC2231 – Internet Systems and Services

Paper Review – TCP Congestion Control with a Misbehaving Receiver
Name: Alex Wun

By identifying weaknesses in TCP's RFC specifications, Savage et al. are able to bypass TCP's congestion control behaviours. They specifically demonstrate three techniques: ACK division, DupACK spoofing, and Optimistic ACKing. ACK division increases the sender's transmission window artificially by ACKing at byte granularity rather than segment granularity. DupACK spoofing sends a stream of duplicate ACKs to abuse TCP's fast retransmit algorithm. And Optimistic ACKing tries to acknowledge data that has not been sent yet in order to fake a short RTT to the sender.

This paper illustrates how RFC specifications can sometimes be incomplete or vague. It is often up to the implementer to catch pathological use cases that result in undesirable behaviours. The authors have found an interesting flaw in TCP's RFC specs that could potentially result in DoS-style attacks at the transport level.

However, the authors propose solutions that require a small modification to the TCP protocol – adding nonce fields. Unless the threats are shown to be serious, it's unlikely that the protocol will be modified (a non-trivial task that will require upgrading all TCP services). Savage et al. have shown that exploitation is possible, but have not investigated whether this is a significant problem out on the Internet (the implication is in fact that it's not, even though most operating systems are vulnerable). Also, ACK division seems to be easily preventable in implementation (Linux 2.2) and Optimistic ACKing, if used too aggressively, will result in erroneous transmissions that are useless to an attacker. It's possible to cause a surge in TCP traffic, but if an attacker chose to perform a DoS attack – he would likely take a more traditional application level approach. This casts doubt on whether the discovered flaws (although undesirable) are serious issues.