More Accurate Explicit Congestion Notification (AccECN) Feedback in TCP

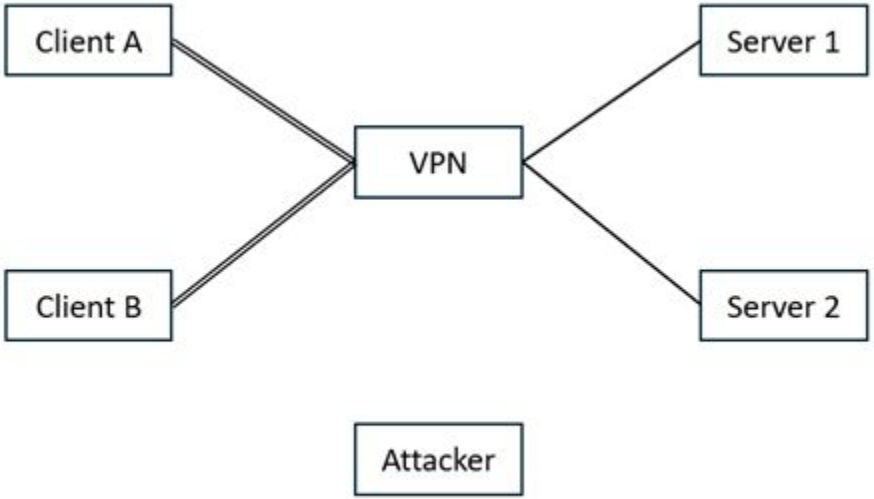
draft-ietf-tcpm-accurate-ecn-34

IETF 124 Montreal - tcpm

Security Considerations Review

- In AD review (last Dec) Zahed provided “Comments on the security consideration section (copied from Christian's review)”
- A new attack was described to identify traffic flows using congestion response
- New text was added to the security consideration section without further discussion
  - Contains an (unclear) description of the attack and a recommendation to disable Accurate ECN
  - However, the attacks already exists with ECN as well as drop and the additional risk that Accurate ECN feedback could introduce by enabling new congestion controls is unclear.

The attack



1- Attacker wants to know which of client A and client B is accessing server 2

2- Attacker tweaks the Accurate ECN field in packets from VPN to server 2.

3- In response to Ac ECN, server 2 reduces its send rate.

4- Attacker observes that the traffic to between A and VPN does not change, but traffic between B and VPN slows down.

5- Attacker has identified B as accessing server 2.

Current text

As Accurate ECN exposes more bits in the TCP header which could be tampered with without interfering with the transport excessively, it may allow an additional way to identify specific data streams across a virtual private network (VPN) to an attacker which has access to the datastream before and after the VPN tunnel endpoints. This may be achieved by injecting or modifying the ACE field in specific patters that can be recognized.

Overall, Accurate ECN does not change the risk profile on privacy to a user dramatically beyond what is already possible using classic ECN. However, in order to prevent such attacks and means of easier identification of flows, it is adviseable for privacy conscious users behind VPNs to not enable the Accurate ECN, or Classic ECN for that matter.

Proposed text

ECN or packet drops enable on path attackers to cause connections to slow down. Accurate ECN can enable a broader set of congestion reactions. If the congestion reaction can be observed at multiple points in the network, this can be used to de-anonymize traffic going through a VPN. However, variations of this attack are already possible with classic ECN, or by simply causing packet loss.