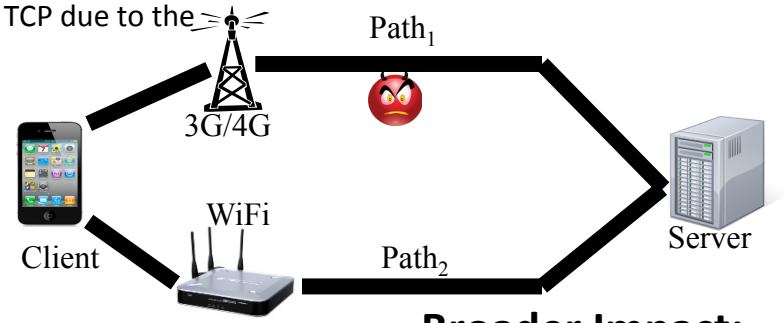
Multipath TCP Traffic Diversion Attacks and Countermeasures

MICHIGAN STATE UNIVERSITY

Alex X. Liu (Michigan State University), **Zhiyun Qian** (Univ. of California – Riverside), **Zubair Shafiq** (University of Iowa)

Challenge:

- Investigate multi-path TCP (MPTCP) attack surface and propose new attacks and defense mechanisms
- Multipath TCP (MPTCP) allows one connection between two hosts to use multiple paths simultaneously
  - For example, smartphones can stream video over both WiFi and 3G/4G connections simultaneously
- Larger security attack surface than TCP due to the use of multiple paths



Solution:

- We present two novel practical attacks on MPTCP, traffic diversion attacks and hijack attacks using
  - throughput information obtained from global sequence numbers, and
  - the MPTCP MP_PRIO option
- We reason about the desired security properties and propose two countermeasures to prevent traffic diversion and connection hijack attacks
- Our solution is based on lightweight encryption (leveraging existing MPTCP key material)

Scientific Impact:

- Lack of prior work on analyzing and comparing the attack surface of MPTCP with that of TCP
- Demonstrates that new attacks are possible and old TCP attacks (e.g. connection hijacking) can be more easily launched on MPTCP
- Helps understand, what security guarantees are desired of MPTCP and what security mechanisms should be provided at the MPTCP

Broader Impact:

- Our work exposes possible implications of MPTCP security flaws on network operators and public users
- A malicious network operator (or user) can use proposed attack to
  - divert traffic to other networks to save its own bandwidth
  - hurt performance of other network users
- Proposed solution can be integrated with MPTCP to make systems and devices more secure