draft-per-app-networking-considerations-00

Lorenzo Colitti, Tommy Pauly

Motivation

- Lots of interest recently in application-based networking (APN6, …)
- Draft briefly discusses some of the implications

Per-application networking use cases

- Mobile devices usually connected to more than one network at a time
  - e.g., VoLTE + cellular data + Wi-Fi captive portal

- Network operators/applications may want traffic to be sent on other network
  - Resources on a network that does not have Internet access
    - (VoLTE, IMS/RCS, airplane entertainment system)
  - Enterprise network (e.g., “backend” circuit separate from Internet access for PoS terminal app)
  - Specific performance requirements (e.g., voice app traffic scheduled/queued differently)
  - Zero-rating traffic (e.g., “free video streaming traffic” bundle)
  - Local breakout (e.g., use IPv6 addresses that are local to a specific area, and do not have wide mobility)

Implementation

- Today, In commercial/public networks this is often implemented via DPI
  - e.g., flow tracking + SNI handshake inspection
- Problems with Deep Packet Inspection
  - Complex
  - Policy concerns
  - Rendered ineffective by continued move towards encryption (RFC 7258…)
- Alternative: host chooses what network to send traffic on
  - diffserv, PvDs, APN6, Network tokens, 5G slices, ...
- This draft explores the implications, and suggests mitigations

Open Internet implications

- Could be used to discriminate between types of traffic
  - In some jurisdictions, networks cannot discriminate based on application
- If network has influence on host (e.g., mobile carrier requirements), host impacted as well
- Can be mitigated or avoided by discriminating between traffic classes instead of between different applications
- May be mitigated if user is aware of special treatment

Privacy implications

- Some proposals say that app should expose its identity to the network
  - RFC 7258 says network protocols should expose least information possible
  - Information about what applications in use is highly privacy-sensitive
- Identity can be exposed even even in the absence of explicit signalling
  - e.g., host sets policy that requires app X to be on network Y
  - Network Y can evince that app X is in use because it sees a packet
- Can be mitigated or avoided by discriminating between traffic classes instead of between different applications
- Can be mitigated if user is aware of privacy implications?

Other considerations

- Categories must be broad enough not to identify individual applications
  - Example: role-playing game:
    - Role-playing game?
    - Game?
    - Real-time/low-latency?
    - Internet traffic?

- Should have APIs for this that are not tied to specific signaling technologies
  - Selecting a Provisioning Domain (PvD) might be a useful layer of abstraction
  - API should not reveal user identity to the network without network authentication

Questions?