Privacy considerations for DMM

Charlie Perkins
Sri Gundavelli

IETF91 Honolulu

12nd November 2014

Overview

- Need for the draft – what is the threat?
- DMM design phase must consider implications of identifier persistence
- Known privacy considerations
- Some solution approaches
- Next steps?
  - a gap analysis?

Need for the draft

- Recent awareness of privacy issues for many Internet protocols
- Persistent identifiers can enable tracking
- cookies can be correlated with other information
- DMM requires security; security is typically based on some sort of identifier or cookie
- Mobile IP solutions have also enabled visibility of identifiers within tunnels / redirections

DMM design phase

- Now is the time to discuss the issues
- Does not necessarily have to fit in the architectural diagrams, but architecture needs to be realistic if identifiers are not persistent

Known privacy considerations

- Trackable identifiers
- Confidentiality for sensitive identifiers
- Other non-privacy security matters not covered in the draft (e.g., non-repudiation)

Some solution approaches

- Pseudo-home address feature [RFC5726]
- Short-lived source IPv6 address for data
- MPTCP for protection against traffic analysis
- MAC randomization
  - Generating Opaque IIDs with SLAAC [RFC 7217]
  - Apple announcement
  - Privacy EC SG in IEEE 802 studying the issues
  - ietf-PrivRandMAC SSID

Next Steps

- Solicit inputs from WG and from task groups

Future work

- Add more privacy threats
- Include more privacy-enhancing solutions possibly useful for DMM design phase