Privacy Extensions for DNS-SD

Christian Huitema
IETF95, Buenos Aires
Monday 4th April 2016
Privacy: stem the flow of metadata
Don’t feed the critters

- MAC Addresses (Randomization)
- DHCP parameters (Anonymity)
- DNS Traffic (DNS Privacy)
- MDNS
  - Host name
- DNS-SD
  - Service name
  - Host name
DNS Privacy is not enough

• D-Prive, DNS over TLS
  • Protect privacy of requests
  • Relies on trusted resolver

• DNS-SD issues:
  • Publishes A/AAAA record for name
  • Publishes service name at location

• DNS Privacy does not protect publisher
Proposed solution: obfuscation

• Publish random name with MDNS
  • Defeats tracking by host name
  • No impact on “list picker” interface

• Publish obfuscated service name
  • `<base64_seed> "." <base64_hash>`

• Publish Instance/Key pairs to friends (similar to Bluetooth)
  • Instance = “Alice’s Picture Store”
  • Key = EF0123456DEADBEEF

• Friends can discover the service
This is V0, there are issues

• Key distribution
  • Probably OK in single owner “laptop to phone” scenario
  • Could use process similar to Bluetooth

• Goobledygook
  • Non friends see strange looking strings in “list picker”

• DOS Attack
  • Publish lots of goobledygook, force lots of computation by discoverers

Discuss?