Prototype Implementation

• Developed by Nick Grifka on test version of Windows 10 (not in the product yet)

• Implemented both DHCPv4 and DHCPv6 versions
  • Straightforward
  • Implementation choice: do not send Host Name, FQDN
  • Needed variance on DHCPv6 CONFIRM – performance issue

• Alternate behavior triggered by use of Random MAC Address

• Additional complexity is modest
Trials in the wild

• Tested on 9 different Wi-Fi hot spots in Bellevue / Seattle area
  • Ranged from big brands (ATT Wi-Fi, Google) to cafes and public library
• Connection (almost) always succeeded
  • One exception: Wi-Fi network did not allow connection using randomized MAC Address.
  • DHCP profile itself did not cause any failure
• Confirms validity of “No Name” option
  • DHCP servers do not actually need the name of your device
  • Changed draft to “SHOULD avoid sending the host name option.”
Summary of changes

• Section 2.6. Using the anonymity profiles, static vs. mobile.
• Section 3.4. Client Identifier Option, for PPP links
• Section 3.5. Default to not sending Host Name
• Section 3.5. If sending Host Name, obfuscate, don’t leak MAC Address
• Section 4. Prefer Stateless IPV6 address configuration when possible
• Section 4.1. Allow DHCPv6 CONFIRM when roaming between Access Points
Next step?

- Do we need anything more before last call?
Background slides
History

- Presented draft-huitema-dhc-anonymity-profile at IETF 92, Dallas.
- Revised with Tomek Mrugalski, Suresh Krishnan
- Adopted by WG.
- Version 01 published June 30, 2015
- Feedback from mailing list, implementation, trials
- Version 01 published June 30, 2015
Feedback on DHCPv6 Confirm

• Found one issue with DHCPv6 CONFIRM
  • Used when roaming between access points
  • Code has logic to recognize “same network” using Wi-Fi authentication
  • DHCPv6 CONFIRM allows for continuous connectivity, instead of full DISCOVER/REQUEST cycle.

• Updated draft to allow CONFIRM when roaming between wireless AP in same network.
Feedback: different networks, use cases

• Some networks do not use “link layer addresses,” users still need privacy:
  • Added text in section 3.4. Client Identifier Option
  • Suggestion: Pick random identifier, unique to current link.

• Case of “shared allocation” (draft-ietf-dhc-dynamic-shared-v4allocation):
  • Added text in section 2.6. Using the anonymity profiles
  • Distinguish between “stability for static clients” and “privacy for mobile clients”
Feedback: don’t leak the random MAC

• Previous version suggested constructing an “anonymized host name” as HEX rendering of Random MAC Address.

• Problem: names leak outside the scope of the link, and leaking MAC Addresses outside of their scope increases the attack surface.

• Changed the suggested construction to “HEX of Hash(secret, MAC)”
Feedback: for DHCPv6, prefer stateless

• Feedback expressed during IETF 92, incorporated in draft 00:
  • ... When these options enable stateless address configuration hosts using the anonymity profile SHOULD choose it over stateful address configuration...
Feedback on DHCPv6 Confirm

• Found one issue with DHCPv6 CONFIRM
  • Used when roaming between access points
  • Code has logic to recognize “same network” using Wi-Fi authentication
  • DHCPv6 CONFIRM allows for continuous connectivity, instead of full DISCOVER/REQUEST cycle.

• Updated draft to allow CONFIRM when roaming between wireless AP in same network.