DHCP Privacy Considerations

draft-ietf-dhc-dhcp-privacy-00
draft-ietf-dhc-dhcpv6-privacy-00
draft-mrugalski-dhcpv6-privacy-mitigation-00

Christian Huitema, Sheng Jiang, Suresh Krishnan, **Tomek Mrugalski,** Bernie Volz

Analysis drafts

- Adoption call successful in January for draft-jiang-dhc-dhcp-privacy-00, draft-krishnan-dhc-dhcpv6-privacy-00
- Published as draft-ietf-dhc-dhcp-privacy-00, draft-ietf-dhc-dhcpv6-privacy-00
- Std => Informational
- Next steps
  - Anything else you want to be covered here?
  - Wait for the mitigation drafts to mature?
  - WGLC and publish?

Mitigation drafts

- draft-huitema-dhc-anonymity-profile-00
  - Client does not trust the network (including the server), limit disclosure of any information
  - Ok to sniff, because there's nothing useful to sniff
  - Will be covered by separate presentation
- draft-yiu-dhc-dhcpv6-sa-00
  - Client trusts the server, server-client communication may be encrypted => confidentiality
  - Will be covered by separate presentation
- draft-mrugalski-dhcpv6-privacy-mitigation-00
  - Collection of mitigation ideas, will evolve into solution

draft-mrugalski-dhcpv6-privacy-mitigation-00

- Exploratory draft, see what's on the table, not necessarily turn everything into proposed solution
- Expected to evolve significantly
- Significant overlap with draft-huitema-dhc-anonymity-profile-00
- Will merge those two

Section 3.1: Not disclose the desire for privacy

- Client could signal its desire for privacy
  - Pro: cooperating server could enable extra privacy features
  - Con: operators participating in surveillance and anti-privacy (willingly or not), can enable additional surveillance mechanisms
- Client does not reveal his desire
  - Pro: much harder indistinguishable from server's perspective
  - Con: … ?

Already in –anonymity-profile-00, no action needed

Section 3.2: Randomized DUIDs

- Could define new DUID type: random
  - Con: would disclose the desire for privacy
- Client could randomize its DUID…
  - Must be closely coupled with MAC randomization
  - Every time it connects to a network
    - Super privacy
    - Excessive resources usage
  - Every time it connects to a new network
    - Prevents movement tracking (makes correlation difficult)
    - Network-to-duid mapping maintained by a client
  - Over time
- Should randomize the whole DUID (including OUI)?

Already discussed in –anonymity-profile

Section 3.3: Don't send Confirm

- RFC3315 says to send Confirm when location may have changed
- Confirm = "Hey, this was my previous location"
- Recommendation:
  - Do no send Confirm
  - Do not send existing leases in Solicit
  - Pro: not reveal previous location
  - Con: link flap will restart configuration process

Not mentioned in –anonymity-profile, will merge

Section 3.4: Temporary addresses

- By using IA_TA, the client indirectly reveals its desire for privacy
- Proposal:
  - Not use IA_TA
  - Send IA_NA with randomized IAID
  - To enforce address change, send IA_NA with new IAID before releasing the old one

if there's consensus, will add to –anonymity-profile

Section 3.5: Avoid FQDN

- Client may reveal its (previous) hostname by sending client FQDN option
- Privacy and disclosing one's hostname and address in DNS do not play along well
- If DNS entry is needed for whatever reason, use randomized hostname

Already covered in –anonymity-profile

Section 3.6: Randomize order

- Options order may be used to fingerprint the client (OS, client software, version etc.)
- Randomize options order in the message
- Randomize options codes order in ORO

Not covered in –anonymity-profile, will merge

Section 3.7: Anonymous inf-request

- Sending client-id in INF-REQUEST is optional
- Don't send it

Not covered in anonymity-profile, will add

Server privacy mitigation

- TBD

Next steps

1. Refine proposed ideas, throw away useless ones, add others
2. Merge into huitema-dhc-anonymity-profile

Thanks