DHCP Privacy Considerations

Tomek Mrugalski
IETF90, Toronto
2014-07-23

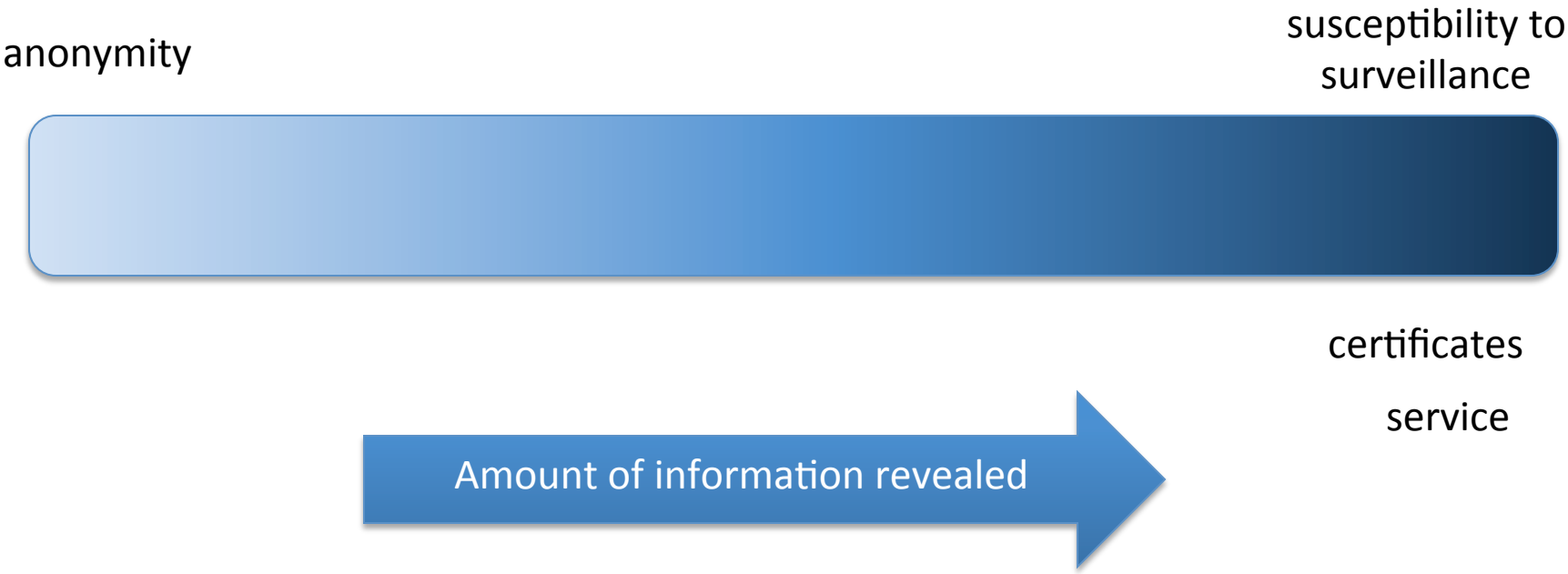
Problem statement

- DHCP is susceptible to surveillance
- DHCP can be used to track users and devices
- Users' mobility patterns may be revealed
- Users' personal information may be revealed
- ...

Examples

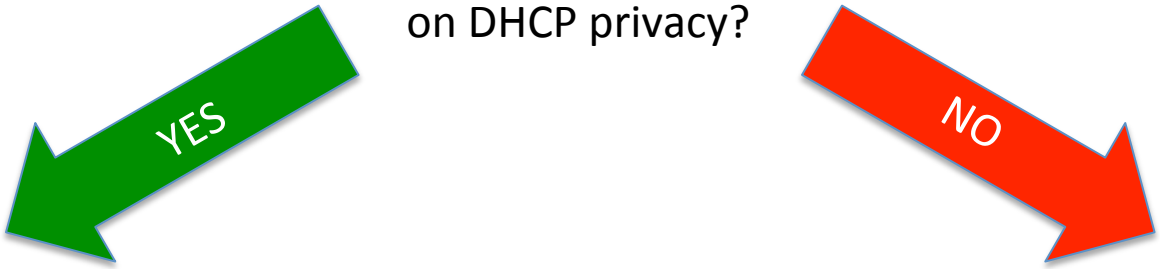
- When moving to a new location, the client sends Confirm with addresses that reveal previous location
- You may be identified by MAC, link-local, DUID, FQDN and many others
- Your device can be fingerprinted by options presence, options content, options order, and behavior
- IA_TA (temporary addresses) will help, but only a little.
  (corresponding servers can track me => my DHCP server can track me)

Privacy vs security

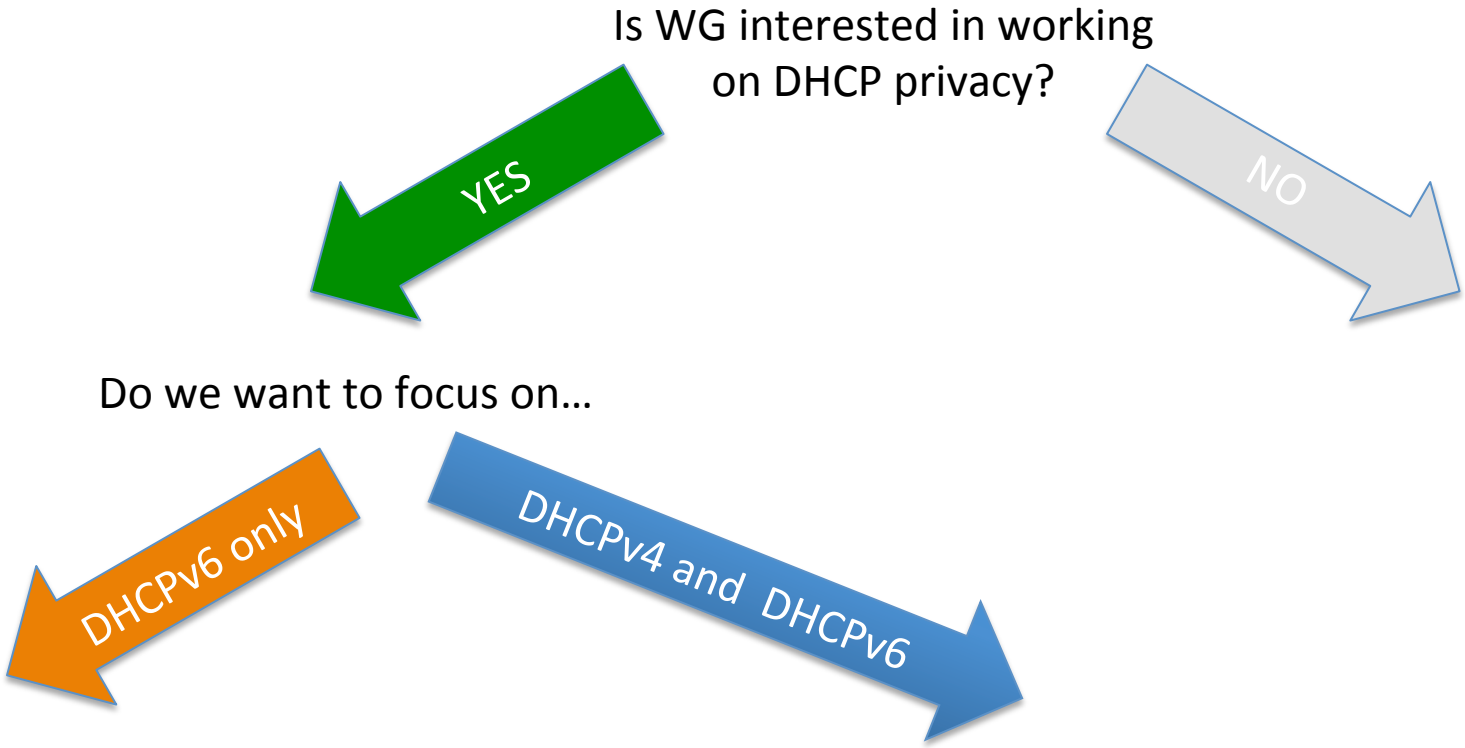


Question #1

Is WG interested in working on DHCP privacy?

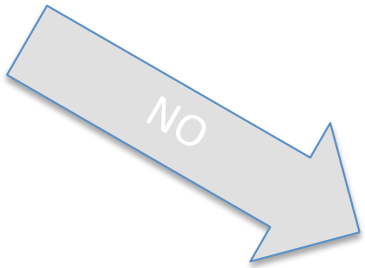


Question #2

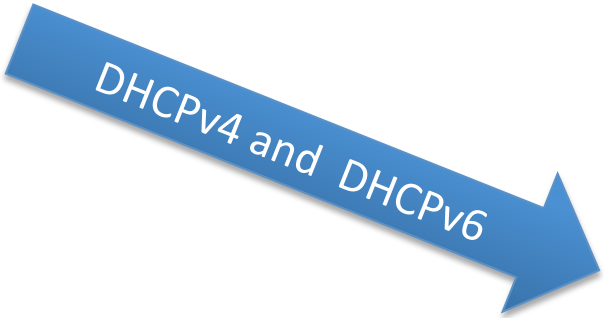

Is WG interested in working on DHCP privacy?
YES
NO
Do we want to focus on…
DHCPv6 only
DHCPv4 and DHCPv6

Question #3

Is WG interested in working on DHCP privacy?



Do we want to focus on…



What should our goal be?

- Analyse
- Analyse and change protocol if needed
- Analyse and decide what to do next

Question #4

How much would you like this work to proceed?

Not much
(honestly I don't care)

A bit
(I will discuss and review)

A lot
(I volunteer for this work)

Scope of work

- Part of a bigger picture
  - Much bigger problem than just DHCP
  - Need to limit the analysis to DHCP aspects only
- Problem analysis
- Discussion of possible solutions
- Review existing drafts and comment on privacy implications

Next steps?

Further reading

No.	Title	Reason
1.	RFC7258: Pervasive monitoring is an attack	Why pervasive monitoring is a problem
2.	dhc-v4-threat-analysis-03	What are the potential attacks in DHCPv4
3.	dhc-sedhcpv6-03	Proposed strong protection against attacks, privacy degradation (certs)
4.		