DNSSD Privacy Scenarios
Scenario 1: Coffee Shop Printer

Server is public, client is not.
Requirement:
Do not disclose client’s identity
Scenario 2: Coffee Shop Meeting

Nothing is public.
Requirement:
Do not disclose client’s identity, server identity, or service type
Scenario 3: Wearables

Nothing is public.
Requirement:
Do not disclose client’s identity, server identity, or service type

Taking notes:
David’s watch talking to phone
Privacy and authorization, 2 approaches

• Privacy requires some kind of secret
  • Obfuscate or encrypt queries, announces, responses

• Secret may or may not be used for authorization

• Two models:
  • Secret Identifies the Client (as in DNSSD privacy/pairing draft)
  • Secret provides light weight “discovery” filter, authorization happens once connection is established

• Issue:
  • Different applications have different authorization frameworks
  • Light weight mechanism may be more acceptable