DNSSD Working Group

DNS-SD Privacy
Stuart Cheshire, Apple

100th IETF, Singapore, November 2017
DNS-SD Privacy
Drafts by Christian Huitema & Daniel Kaiser

Privacy Extensions for DNS-SD

Device Pairing Using Short Authentication Strings

Device Pairing Design Issues
• https://tools.ietf.org/html/draft-ietf-dnssd-pairing-info-00
Privacy-Preserving Service Discovery
Much Activity in this Area

Work by Christian Huitema & Daniel Kaiser
Apple AirDrop — contacts only mode
Apple HomeKit — finding your home accessories
Google Nest accessories (IEEE 802.15.4 mesh networking)
Zigbee dotdot

Two other confidential projects
One abandoned project from five years ago
  • Patent just granted — IPR disclosure requested
  … and probably many more
Private Discovery Threat Considerations
draft-cheshire-dnssd-privacy-considerations-01

Outlines privacy considerations
- What operations are protected
- Trust granularity
- Desirable security properties
- Other operational requirements
Private Discovery Threat Considerations
What Operations are Protected

Offer
• Device offers service on network

Discover
• Client discovers what service instances are available

Use
• Client makes use of a particular service instances
Private Discovery Threat Considerations

Trust Granularity

Per physical device?
Per human user?
Per app?
Private Discovery Threat Considerations
Desirable Security Properties

Authenticity & Integrity
Confidentiality
Anonymity
Resistance to Dictionary Attacks
Resistance to Tracking
Resistance to Message Linking
Resistance to Denial-of-Service Attack
Private Discovery Threat Considerations

Other Operational Requirements

Power Management

Protocol Efficiency

Secure Initialization