Private Service Discovery
draft-bradley-dnssd-private-discovery-00

Bob Bradley (bradley@apple.com)

DNSSD
IETF 103, November 2018, Bangkok
Problem

Bonjour service advertisements leak information about devices or users

- Types of services, names, persistent identifiers, etc.

**Goal:** Bonjour functionality between friends without compromising on privacy

Long-term peer key sharing and pairing is out of scope
Protocol Overview

Peers **search for friends** via multicast probes, and friends respond with unicast responses to establish shared secrets.

Peers **advertise availability** via multicast probes, and friends respond with unicast responses to establish shared secrets.

**Shared secrets** are used to encrypt normal mDNS messages.
Probe+Response

Alice

Probe
EPK1 || TS1 || SIG1

Eve

Derive SSKs

Response
EPK2 || ESIG2

Bob

Derive SSKs
Advertisement+Response

Announcement: EPK1 || TS1 || SIG1

Response: EPK2 || ESIG2

Derive SSKs
Query+Answer

Queries are normal DNS messages (PTR, SRV, etc.)

Answers are encrypted answers

```
Alice                          Bob
Query                          Answer
EMSG1-n                        EMSG2-n
Update nonce                   Update nonce
```
Key Schedule

x25519 [RFC7748] for key exchange using ephemeral public keys

HKDF with SHA-512 [RFC5869] for secret derivation
Encryption

Implicit and synchronized nonces between peers

- Makes replay trivial to detect
- Does not deal well with packet loss*
- Out-of-order packet processing requires trial decryption
Open Issues

Should responders send fake replies to non-friends to mask relationships between real friends? (Reaction attacks)

Should peer verification order be randomized to hide contents of friends list?

Do we need versioning? What about agility?

Do we accept the DoS risk?
Questions?