DNSSD Privacy & DNSSD Pairing

Christian Huitema, Daniel Kaiser
draft-ietf-dnssd-privacy-02, draft-ietf-dnssd-pairing-02
IETF 99, Prague, July 2017
DNS-SD Privacy summary

2345XA0F are you here?

Yes, contact me at this address

DNS over TLS exchanges

Damn. I have no idea who says what to whom

This hash matches Alice’s key
DNS SD Privacy

- Prototype implementation
- WGLC, Reviews
  - Stephane Borzmeyer
  - Ted Lemon
- Revision -02
  - Answers Stephane’s review
Issue: Use of PSK

- **Issue:**
  - Design uses shared secrets between pairs of nodes
  - Why not use a public key solution instead?

- **Rationale**
  - Public key is a unique identifier
  - Public key of server is disclosed during TLS handshake => Leak!
  - PSK provides implicit client authentication, access control

- **Proposed Resolution**
  - Will check the design section to ensure that the rationale is clearly explained.
Issue: Time synchronization

• Issue:
  • Nodes publish instance name = hash (24 bit time, shared secret)
  • This requires synchronization to about 4 minute interval
    • Time based nonce controls computing load, mitigates DOS attacks
  • What about the edges of the interval?

• Mitigation implemented in prototypes
  • Accept both current and previous or next nonce

• Resolution
  • Better documentation of edge condition in draft-02
Issue: Time based token and DNS-SD

• Issue
  • Token based on 256 seconds intervals
    • Short interval limits the time opportunity for replay attacks
  • Requires explicit DNS-SD updates every 256 seconds
  • May cause too much load on DNS servers

• Suggested Mitigation (Ted)
  • Specify a longer interval, e.g., 32,768 seconds (about 30minutes)
  • Would still mitigate replay attacks “somewhat”

• Resolution
  • Maybe. Discuss.
Issue: list of ID and fingerprinting

- Issue
  - Each node publishes as many instances as it has pairings
  - Counting the number of instances may allow fingerprinting

- Mitigation tried in prototypes
  - Pad with fake instances
  - Minimal cost for peers who will not resolve the fake instance names

- Proposed resolution
  - Document attack and mitigation in security section
Issue: hostname versus service name

• Issue
  • Draft specifies DNS-SD based discovery, using instance names
  • Many services such as SSH just use host name and port, won’t work easily

• Mitigation, implemented in prototype
  • Perform discovery of the private discovery service
  • Once discovered, securely resolve hostname._private.local
  • Cache results to allow connections to hostname:port

• Proposed resolution
  • Document host name caching?
DNS SD Pairing

• Discovery
  • Potential peers discover each other
  • Two methods: MDNS or QR code

• Key agreement
  • Establish TLS connection using TLS and [EC]DH Anon
  • Each node exports the key from TLS context

• Verification to defeat MITM
  • Commit hash(nonce), compute short string = hash(nonce, key)
  • Verify same string displayed on both sides (text or QR code)

• Remember the secret associated with the pairing
DNS SD Privacy

- Prototype implementation
- WGLC, Reviews
  - Thanks, Ted.
- Revision -02
  - Clarifications

- Review issues:
  - Clarify discovery (SRV/TXT for presence service)
  - QR code
  - Separate analysis and spec
Issue: separate QR code specification

• Issue
  • Draft specifies QR code option as alternative for discovery and verification
  • “This feels like a separate protocol”

• Motivation
  • QR code verification is widely used in existing systems, e.g. Signal app

• Proposed resolution
  • Need feedback from the list
  • Could move QR code verification to separate document
Issue: separate analysis and text

• Issue:
  • Pairing draft includes lengthy discussion of requirements and potential solution
  • Results in large document, when spec itself is fairly short
  • Implementers more comfortable with short spec
  • Separate analysis could be reused by HomeNet

• Proposed resolution, pending WG agreement
  • Split pairing into two drafts, informational analysis and standard track protocol
Next steps?

- Private discovery passed WGLC, is ready
- Pairing passed WGLC but
  - Could split analysis, specification, and QR code
  - Would probably need second WGLC for pairing