mDNS/DNS-SD & ULAs

DNSSD WG IETF-90

Douglas Otis

mDNS/DNS-SD Security

- mDNS security is premised on multicast constrains ensuring devices are local
- DNS-SD publishing routable addresses offers **NO** locality constraint
- Firewall protection depends on constraining non-local session initiation
- draft-ietf-homenet-arch-17#section-3.6.6 ULAs as a hint of connection origin
- ULAs can thwart:
  - unintended data exfiltration
  - external traffic infiltration
  - encapsulation/injection spoofing techniques

ULAs offers security for mDNS Hybrid DNS-SD

```
FC00::/7 |L| Global-ID      | Subnet-ID | Interface-ID
7 bits   |1| 40 random bits | 16 bits   | 64 bits
```

- FD00::/8 clearly indicates locally defined addresses
- ULAs provide a means to support firewall rules or split-horizon DNS
- All-in-One printer/scanner/fax/media-readers may return routable address in mDNS but should not be directly accessible from the Internet
- Devices unable to authenticate a session should not have their address published in DNS as this still exposes their Interface-ID
- Many unpatched devices have known exploits; and for many no patch was ever made

DNS not Confidential

- Split-Horizon deployment offers limited protection of DNS-SD discovery resources normally based on the DNS query source IP address

- Not being able to differentiate device locality to handle Internet originating sessions, such as that for a printer, suggests Scalable DNS-SD/mDNS extensions can not be safely managed nor kept confidential

- See RFC6950 Private DNS and Split Horizon

- Information may leak via caches, search engines, etc.

Copy Protected Links

- Sept 2010 HDCP Master key compromised
- With easily subverted link protection, HDCP enforcement seems largely based on threat of litigation
- Locality tests: static topology and RTT of less than 7ms
- Within large environments, ULAs having locally defined Global-IDs also limit possible distribution
- AppleTV will soon support wireless peer-to-peer control; layer 3 routing not supported and soon not needed

ULAs offers DNS Stability

- Multiple IPv6 prefixes and reassignment is a reality
- DNS/DNS caching will cause service disruptions when ULA overlay networking is not used
- ULA overlay provides stable, secure, conflict free remote access such as that used with BTMM
- New TLDs and PseudoTLDs growth makes local namespace use difficult to ascertain or properly resolve
- Granting exceptions for use of UTF-8 labels becomes fairly impractical without use of ULAs

“Distrust and caution are the parents of security.”

– Benjamin Franklin