Scalable DNS-SD (SSD) Threats IETF94

Review

Terminology

- Realm Namespace
  - A realm specific namespace accessible for resolution referenced from a subdomain that may not be within the root domain
- Local Namespace
  - A namespace accessible for link-local resolution that may be referenced from an Ambiguous Local Qualified Domain Name (ALQDN) representing a network segment or broadcast domain

Visual Spoofing

_<sn>._<Proto>.<SrvDOM>.<ParentDOM>

To better ensure local namespace is properly handled, alternative zones might replace ASCII punctuation and spaces in SrvDOM labels with the '_' character except when located as the leftmost character

This '_' substitution should reduce visual confusion of parent domains and reduce string handling issues

Restricted Distribution of Sitelocal Addresses

ULA or **[RFC1918]** addresses are less likely routed beyond the site

Other Resource concerns include hostnames, MACs, networking details

Leaking sensitive information might grant malefactors access

Not publishing sensitive information in global DNS reduces exposure to the Internet

Resource Exhaustion

_services._dns-sd._udp.<Domain> PTR RRset

Can change notification facilitated with **[I−D.ietf−dnssd−push]** based on TCP that uses message structure defined by **[RFC2136]** be able to replace meta-query UDP DNS browsing?

Alternatives are DNS RRL (Response Rate Limiting)

http://www.redbarn.org/dns/ratelimits

[I−D.ietf−dnsop−cookies] reduces reliance on DNS Response Rate Limiting and resources needed to handle random initial exchanges in a manner as described by **[RFC6013]** for forged sources of initial TCP <Syn> where servers retain client state in encrypted cookies

Issues not covered?