Domain Boundaries in DNS Zones

Andrew Sullivan & Jeff Hodges

DBOUND at IETF 89

Why do this?

- DNS names are used to build policies
- That’s not great
  - Admin relationships are crudely represented in external-to-DNS systems

Examples

- HTTP state management aka “cookies”
- User interface indicators
- Setting the `document.domain` property
- Email authentication mechanisms
- TLS/SSL server identities
- HSTS and Public Key Pinning

SOPA approach

- draft-sullivan-domain-policy-authority-01
  - unchanged from -00, just bureaucratic
- Defines “policy realm”
- Start Of Policy Authority (SOPA) RRTYPE
  - Specifies whether a name is *included* in the owner name’s policy realm, or *excluded* from it.
  - Does not allow deep cross-tree linkage

SOPA declarations (1)

- "Nothing is in the same realm as me."
  - Just like the public suffix list, only dynamically updatable
- "This [descendant|ancestor|sibling] name is in the same realm as me."
  - Allows example.com to include www.example.com, and conversely

SOPA declarations (2)

- “My entire subtree is in the same realm as me”
  - Useful for an apex point that is the start of a policy realm
- “These related names are in the same realm as me, *except for* this other name”

Generic

- SOPA provides a generic mechanism to express relationships
  - Necessary to express relationships
- The “same-tree” restrictions could be relaxed in future if needed