A Background about SubTLDs

draft-pettersen-subtld-structure-10

Yngve N. Pettersen
Vivaldi Technologies AS

Dbound BOF, IETF 89

The Beginning

1994: Netscape defined HTTP Cookies
1998: «Cookie Monster Bug» discovered

HTTP cookies set by malicious.co.uk
can be sent to any domain foo.co.uk,
enabling cookie injection attacks.

Countermeasures

- Require 2 dots in non-generic domain names.
  Problem: parliament.uk, vg.no
- Blacklist of secondlevel domains, such as co.tld
  Problem: Did not include all relevant domains
  Examples: ltd.uk and city.state.us
- Use DNS lookup of parent domain
  Problem: Depend on site DNS configuration
- General problem: False positives and negatives

Public Suffix List

- Gather information from all TLD registries
- Distribute to clients as web service
- Mozilla and Microsoft maintain such lists
- Challenge: Completeness and timeliness

New Direction: Extending DNS

- Benefit: Registries maintain information
- Benefit: Information available directly in DNS

- Challenge: Airgapped networks
- Challenge: DNS APIs in OS?