Organizational Domains and Use Policies for Domain Names

Casey Deccio
Verisign Labs

DBOUND WG Meeting
IETF 94

draft-deccio-dbound-organizational-domain-policy-00

- Motivation
- Organizational Domain and Use Policy (ODUP)
- Policy-negative Realm
- Example Use
- Conclusion

Motivation

- The current primary resources for identifying domain name policy:
  - **Namespace alignment:**

    Are there ancestral relationships?
  - **Publix suffix consideration:**

    Is there public suffix involvement?
- There is a desire to expand the capabilities of policy identification
  - Examples:
    - **HTTP cookies** – cookie accept/send policies, and "Domain" attribute restrictions
    - **DMARC** – identifying organizational domains

Problem Scope

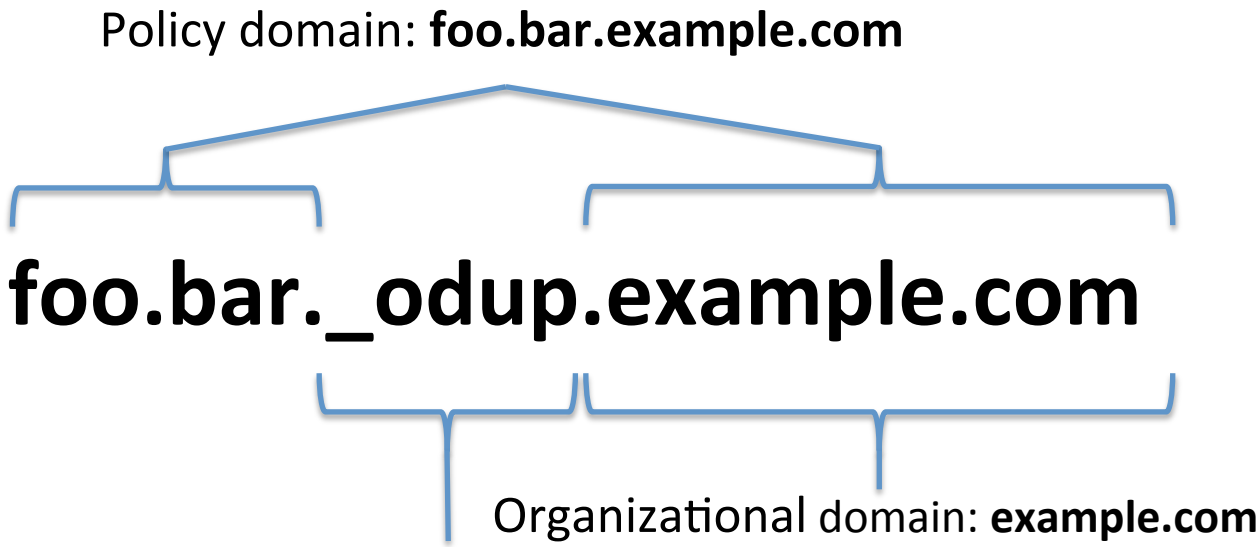
- Hierarchical relationships
  - www.example.com ⇐⇒ example.com
- Cross-domain relationships
  - www.example.com ⇐⇒ www.example.net
- Current draft only addresses first aspect

Organizational Domain and Use Policy (ODUP)

- Designate in-hierarchy:
  - Organizational domains
  - Policy domains
  - Use policy
- Backwards compatible with existing mechanisms and behaviors
- Flexible
- Extensible

ODUP Names

- ODUP name components:
  - _odup label
  - Organizational domain
  - Policy domain



ODUP Policies

- ODUP policies are designated using TXT records at ODUP DNS names
- Zero or more more directives, prefaced by +/- qualifier
- Examples:
  - **httpcookie** – Allowed in “Domain” attribute
  - **tlscert** – Allowed in TLS certificate
  - **wildcardtlscert** – Allowed in wildcard TLS certificate
  - **all** – default policy
- If no “all” directive is used, then “+all” is appended to policy

ODUP Special Directives

- **org** – policy domain is an organizational domain (i.e., delegation of policy)
- **bound** - designates an organizational boundary below the policy domain name

ODUP Resolution

- Input:
  - Domain name
- Output:
  - Policy domain
  - Organizational domain
  - Policy

ODUP Resolution Algorithm

To look up policy for domain name domName:

Begin with the root as the organizational domain (orgDomain).

1. If domName has same number of labels as organizational domain, then return policy at _odup.<orgDomain>.

_odup.foo.bar.example.com

ODUP Resolution Algorithm

2. Form new ODUP name by iteratively adding labels to policyDomain (i.e., below _odup label), beginning with the first label below orgDomain.
3. Query new ODUP name for record of type TXT.

bar._odup.example.com
foo.bar._odup.example.com
…etc.

ODUP Resolution Algorithm

4. If query yields positive response, save record as longest match.
5. If query yields positive response, and resulting record includes “+org” directive, then go to step 10 (start over with policyDomain as orgDomain).
6. If query yields positive response, and response is synthesized from wildcard, and resulting record includes “+bound” directive, then go to step 10 (start over with policyDomain as orgDomain).

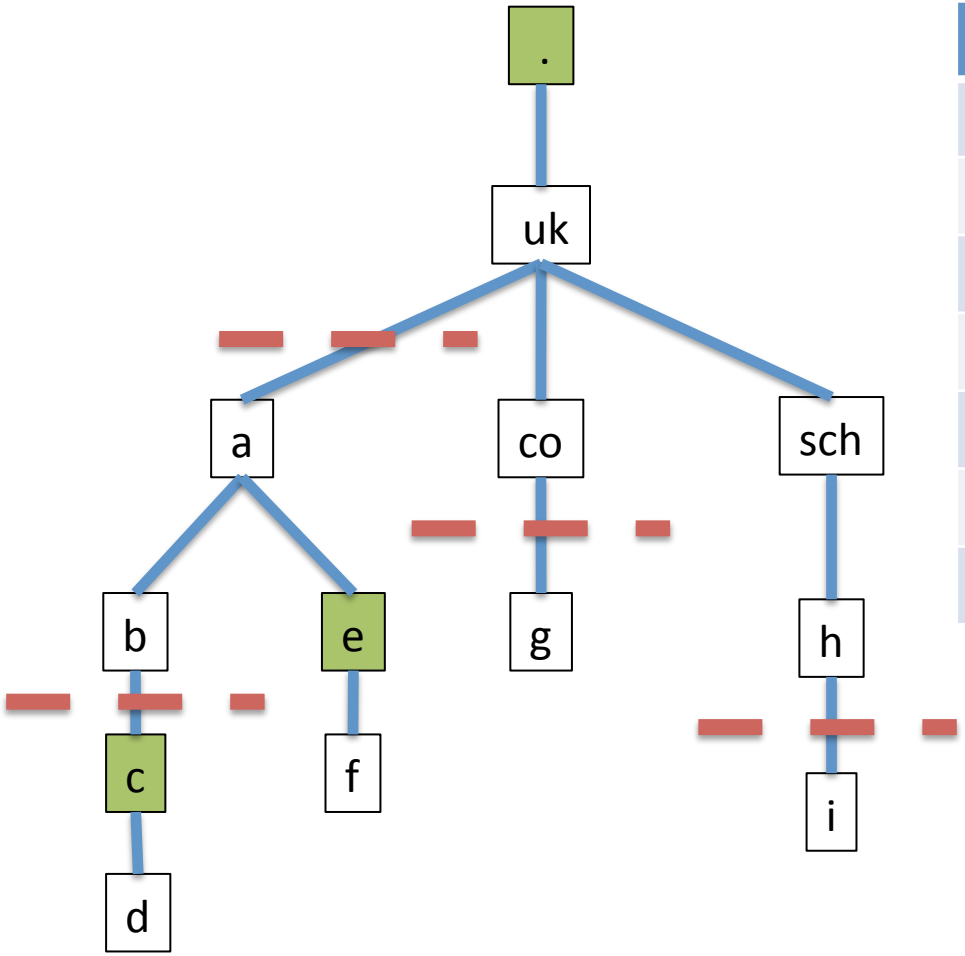
ODUP Resolution Algorithm

7. If query results in NXDOMAIN, go to step 11 (finish).
8. If all labels of domain have been tried, go to step 11 (finish).
9. Return to step 2, increasing number of labels in policyDomain (repeat).
10. If there was no positive response, then return to step 1 using current orgDomain as both policyDomain and orgDomain.

ODUP Resolution Algorithm

11. If the longest matching record includes an "org" directive, then return to Step 1, using the longest matching policy domain as the organizational domain.
12. If the longest matching record includes a "bound" directive, then return to Step 1, using the longest matching policyDomain, plus one label, as the orgDomain.
13. Return the record corresponding to the longest matching policyDomain.

Example

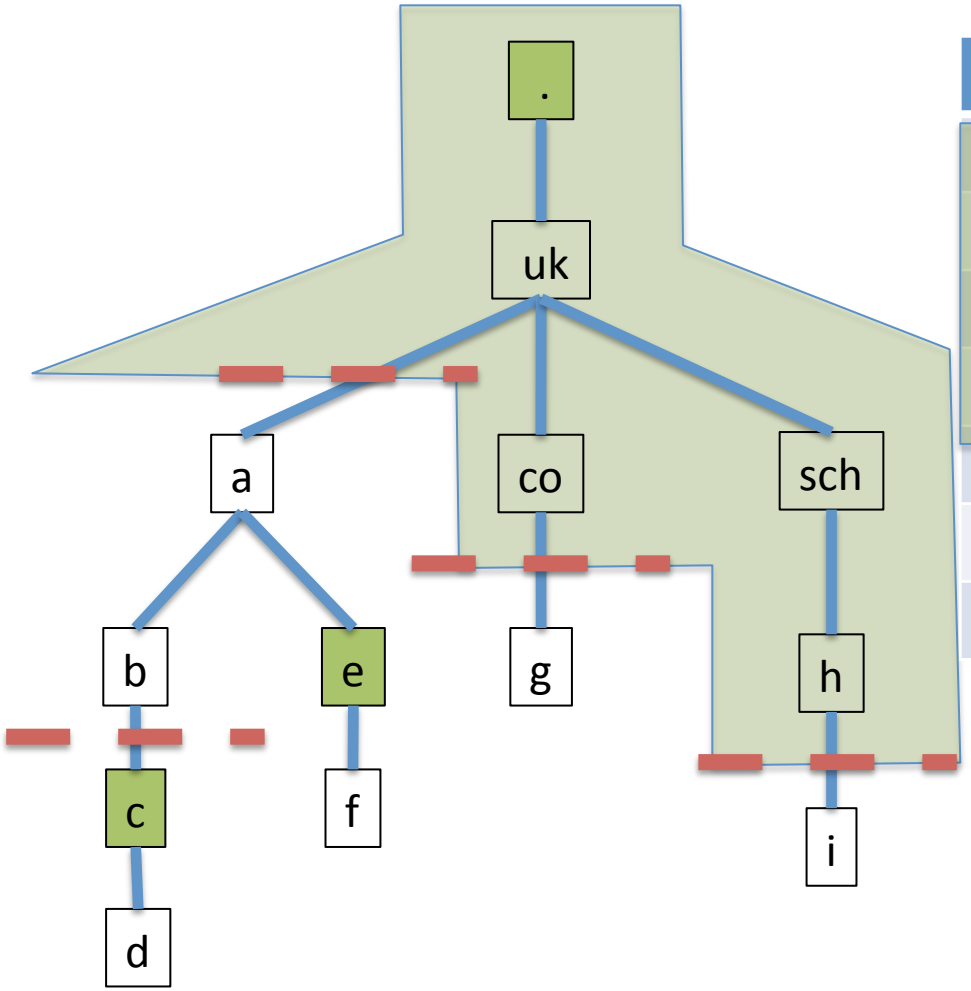


ODUP name	Policy
_odup	-all
uk._odup	+bound
co.uk._odup	+bound
*.sch.uk._odup	+bound
c.b._odup.a.uk	+org
e._odup.a.uk	-httpcookie
_odup.c.b.a.uk	-tlswildcard

Organizational boundaries

e Explicit policy

Policy-negative Realm



ODUP name	Policy
_odup	-all
uk._odup	+bound
co.uk._odup	+bound
*.sch.uk._odup	+bound
c.b._odup.a.uk	+org
e._odup.a.uk	-httpcookie
_odup.c.b.a.uk	-tlswildcard

- Equivalent to PSL (mostly)
- All records within _odup TLD
- Can be accessed via DNS queries or downloaded in its entirety (zone transfer, HTTP, etc.)

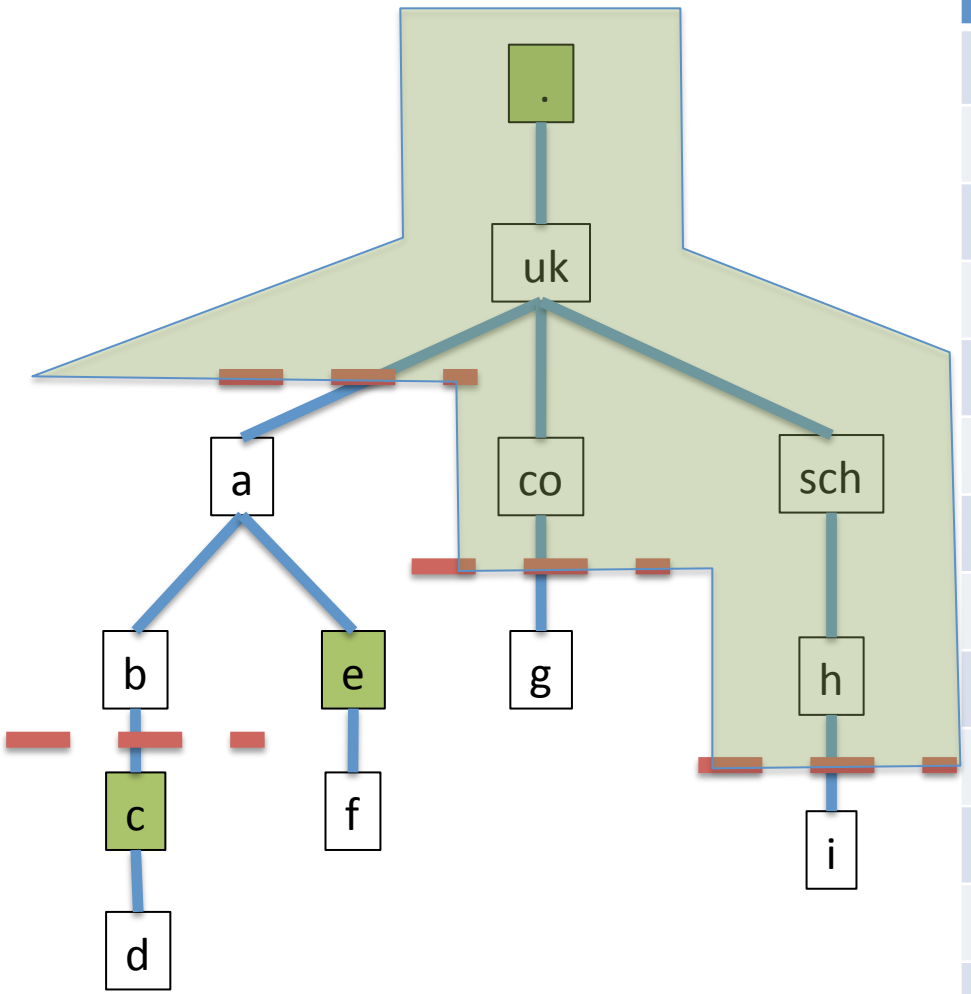
Organizational boundaries

e Explicit policy

Policy-negative Realm

- Name: policy-negative realm is named by its effective policy, rather than using a more abstract categorization such as “public”
- Policy-negative realm designates a boundary, whereas PSL designates public suffixes (subtle distinction)
- TLD doesn’t imply “policy negative” (TLDs aren’t necessarily) public suffixes
- Policy negative realm isn’t constrained by current PSL practices/constraints
  - Any name can be handled outside _odup zone by “delegating” policy using ODUP

Example: Effective Org. Domain

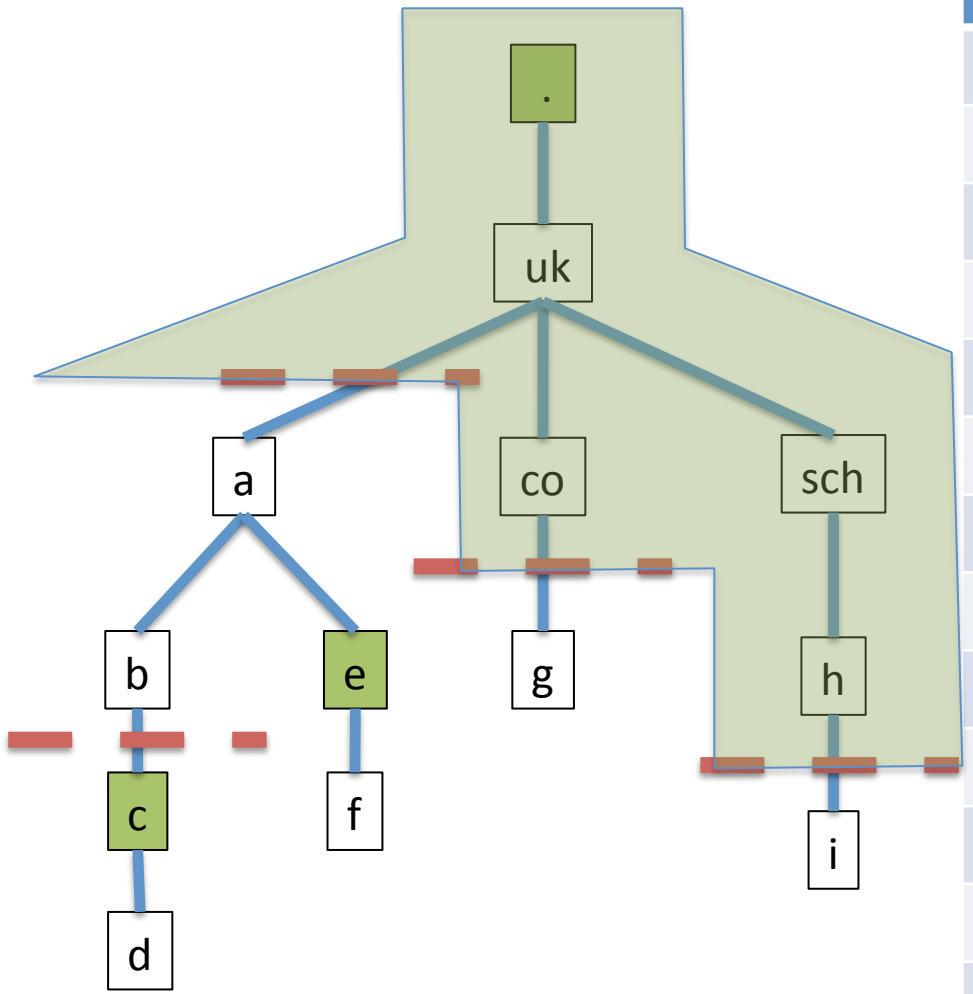


ODUP name	Org. Domain
.	.
uk	.
a.uk	a.uk
b.a.uk	a.uk
c.b.a.uk	c.b.a.uk
d.c.b.a.uk	c.b.a.uk
e.a.uk	a.uk
f.e.a.uk	a.uk
co.uk	.
g.co.uk	g.co.uk
sch.uk	.
h.sch.uk	.
i.h.sch.uk	i.h.sch.uk

Organizational boundaries

e Explicit policy

Example: Effective Policy



ODUP name	Policy
.	-all (E)
uk	-all (I)
a.uk	+all (D)
b.a.uk	+all (I)
c.b.a.uk	-tlswildcard +all (E)
d.c.b.a.uk	-tlswildcard +all (I)
e.a.uk	-httpcookie +all (E)
f.e.a.uk	-httpcookie +all (I)
co.uk	-all (I)
g.co.uk	+all (D)
sch.uk	-all (I)
h.sch.uk	-all (I)
i.h.sch.uk	+all (D)

Organizational boundaries

e Explicit policy

Example: HTTP Cookies

- Cookies cannot be set with a “Domain” attribute by origin servers in different organizational domains than the Domain attribute value.
- Cookies cannot be set with a “Domain” attribute whose policy indicates that setting of cookies is not valid (including policy-negative realm).

Example: DMARC

- Organizational domains other than the one immediately below the policy-negative realm can be designated.

Benefits

- Relatively simple
- Addresses current needs (e.g., HTTP cookies, organizational domain)
- Backwards compatible with current mechanisms
- Policy-negative realm can be accessed either dynamically (DNS queries) or locally (via download)
- Can be made to work offline
- Extensible
- TLD – no longer implies public suffix

Weaknesses

- Requires additional DNS lookup(s) (can be minimized with local copy of policy-negative realm).
- Only addresses hierarchical relationship aspect of DBOUND problem (not cross-domain).

Open Issues

- Wildcards can only be used for single-label synthesis with “bound” directive. Wildcard detection section is wrong in -00 draft and is being re-worked.
- Management of _odup TLD zone needs to be discussed. Draft proposes joint effort between IANA and CA/B Forum.
- Slight changes required to PSL for complete compatibility with policy-negative realm.