Namespace Collisions and Search Lists...

... and lions and tigers and bears! Oh my!

~~Warren Kumari, ICANN Beijing - 2013-04~~
~~Warren Kumari, DNS Inside BB - 2013-06~~
Warren Kumari, ICANN Durban - 2013-08

Disclaimers...

- This is only **one** impact of namespace collisions...
- but it is one of the easiest to explain...
- uses .corp as an example, applies to multiple strings...

Background

- Lots of companies use .corp.example.com for internal stuff
    - Best practice, recommended in many places, including e.g: "DNS Namespace Planning" (http://support.microsoft.com/kb/254680)
- Search list (configured statically, DHCP):
  .corp.example.com
  .example.com

Background

- Users are trained to enter “www.corp” or “fileserver.corp”, “wiki.corp”, etc.
- Many applications configured with names like this (printers, databases, wikis, etc.)
- Buried in code, config files, user habits.

Background

- RFC1535:

```
...
Further, in any event where a
"." exists in a specified name
it should be assumed to be a
fully qualified domain name
(FQDN) and SHOULD be tried as a
rooted name first.
```

Background

- Trying to reach foo.corp:

CLIENT -> SERVER: A? foo.corp.
SERVER -> CLIENT: NXDomain q: A? foo.corp.
CLIENT -> SERVER: A? foo.corp.corp.example.com.
SERVER -> CLIENT: NXDomain q: A? foo.corp.corp.example.com.
CLIENT -> SERVER: A? foo.corp.example.com.
SERVER -> CLIENT: q: A? foo.corp.example.com. A 192.0.2.99

So, what's the problem?!

- Delegations within .corp immediately occludes the internal name space.

CLIENT > SERVER: A? foo.corp.
SERVER > CLIENT: q: A? foo.corp. A 5.5.5.5
~~CLIENT > SERVER: A? foo.corp.corp.example.com.~~
~~SERVER > CLEINT: NXDomain q: A? foo.corp.corp.example.com.~~
~~CLIENT > SERVER: A? foo.corp.prod.example.com.~~
~~SERVER > CLIENT: NXDomain q: A? foo.corp.prod.example.com.~~
~~CLIENT > SERVER: A? foo.corp.example.com.~~
~~SERVER > CLIENT: q: A? foo.corp.example.com. A 192.0.2.200~~

“Solutions” for affected networks

1. Make your internal name-server authoritative for .corp.
2. Make everyone use FQDNs

Option 1
Become auth for .corp

- Cure is worse than the disease.
- Return NXDOMAIN
  - Occludes the .corp TLD
- Return an A record
  - Now you leak cookies every time you go to Starbucks...

Leaking cookies...

- Cookies are used for authentication / single sign-on, etc.
- Cookies are always bound to the FQDN.
- ... so, foo.corp.example.com.
- ... if you make a fake .corp TLD, your **internal** cookie is bound to the **internal** foo.corp.

Leaking cookies...

- Now, when you connect to the **external** foo.corp, your browser will happily send over the cookies...
- now, whoever runs the **external** foo.corp can pretend to be you.

Option 2
Always use FQDN

- Basically impossible
- Humans are creatures of habit
- Various config files have this baked in

FIN.

More reading.

- RFC1535
- SAC045
- draft-chapin-rfc2606bis
- PayPal letter to Fahi and Steve
  - “Proposed Delegation of Invalid Names from SAC 045 and RFC 6762”
- Interisle study.
- draft-kolkman-cautious-delegation