Name Collision Mitigation for Enterprise Networks

Paul Hoffman, VPN Consortium

Name Collision Workshop, March 2014

v1

What's the problem?

- Organizations with **private namespaces** that leak **requests for name lookup** to the global DNS can get **wrong answers**
  - Might or might not be private networks: it doesn't matter
- The shorter version of the problem: **leak**
- This presentation is (mostly) about enterprises doing the mitigation for themselves, not about ICANN doing the mitigation

Primary types of private namespaces

- Names rooted in a **private TLD**
  - On a private network, this makes complete sense if you believe requests will never leak
  - For many years, enterprises creating private TLDs was considered a best practice
- **Shortened names** from global DNS names
  - Also called **search lists**
  - Some still consider using search lists a best practice
  - www.qa has the same problems as mail.corp

The most-proposed solution: don't leak

- **Preventing leaks** would be reliable if:
  - All of the firewalls have reliable, up-to-date DNS proxies
  - There is consistent policy across every firewall
  - No user ever roams outside the protected boundary
- None of those are **realistic** for modern enterprise networks

The next-most-proposed solution: change to another private TLD

- Assuming that the enterprise was using Microsoft Server and/or Active Directory, that would hopefully make sense
- ...until you **look at the documentation** for how to do it
- ...and until you realize that it is just **delaying the pain** and causing a second transition later

Is this really a problem?

- Users sent to unexpected web sites, mail sent to wrong recipients, and so on
- Security reductions due to systems that are relying on the correct resolution of private names
- Yadda, yadda, yadda
- But: the problem is really that organizations are **unlikely to see the problems** or be able to reliably **trace the causes**

There are reliable mitigation plans

- For names rooted in a private TLD: **change names** to use ones rooted in the global DNS
- For networks using shortened names: **stop doing that**
- Neither of these is easy, and both require **deep research** to where the old names (private or shortened) are currently being used

When to mitigate

- Before now, probably a few years ago
- Determining the so-called **“potential for collisions”** for a private namespace is nearly impossible
- Even if the root of someone’s private namespace is not one of the applied-for gTLDs, ICANN might surprise everyone and give “variant” gTLDs that were not applied for

Mitigating for private TLDs in one slide

1. Monitor name requests
2. Create host inventory
3. Find name servers
4. **Change to new names rooted in the global DNS**
5. [Add IPs for TLS]
6. Monitor for name equivalence
7. **Train users**
8. Change hosts to use new names
9. Look for continuing use of old names
10. Long-term monitoring
11. **Point old names at non-functioning address**
12. [Revoke old certs]
13. **Keep serving both names**

Mitigating for private TLDs in one slide

1. Monitor name requests
2. Create host inventory
3. **Train users**
4. Change hosts to use longer names
5. **Turn off search lists in resolvers**
6. Look for continuing use of short names
7. Long-term monitoring

The problem goes beyond enterprises

- A host of peer-to-peer protocols have popped up in recent years
- Many of these protocols have **chosen a namespace** that looks a lot like the DNS, and some even use the DNS protocol
- They don’t appear to care about leakage, but probably should be very concerned

Combining enterprise mitigation and ICANN mitigation (1)

- Enterprises **are responsible** for their network operations
- Every enterprise **has known forever** that ICANN would delegate TLDs that collide with some private namespaces
  - Every new ccTLD probably does this
- The only way for enterprises to not be surprised by ICANN is to **use names from the global DNS**

Combining enterprise mitigation and ICANN mitigation (2)

- ICANN **can choose** to promise to not delegate the obviously most-harmful TLDs, such as .mail and .home
  - Or the IETF can tell them to do so for technical reasons
- The value of ICANN restrictions on SLDs are much less clear
  - We **cannot predict** when a request from a private namespace will leak, or why

Combining enterprise mitigation and ICANN mitigation (3)

- ICANN **not trying to protect** enterprises will certainly cause some damage to enterprises who are using unsafe IT practices
- ICANN **trying to protect** enterprises will certainly cause some enterprises to delay fixing their unsafe IT practices
- ICANN: parent? police? predictable?