RIPE 69- 4 November 2014

DNS Name Collision Risk Mitigation

Brett Carr
Senior Manager, Technical Services
GDD, ICANN

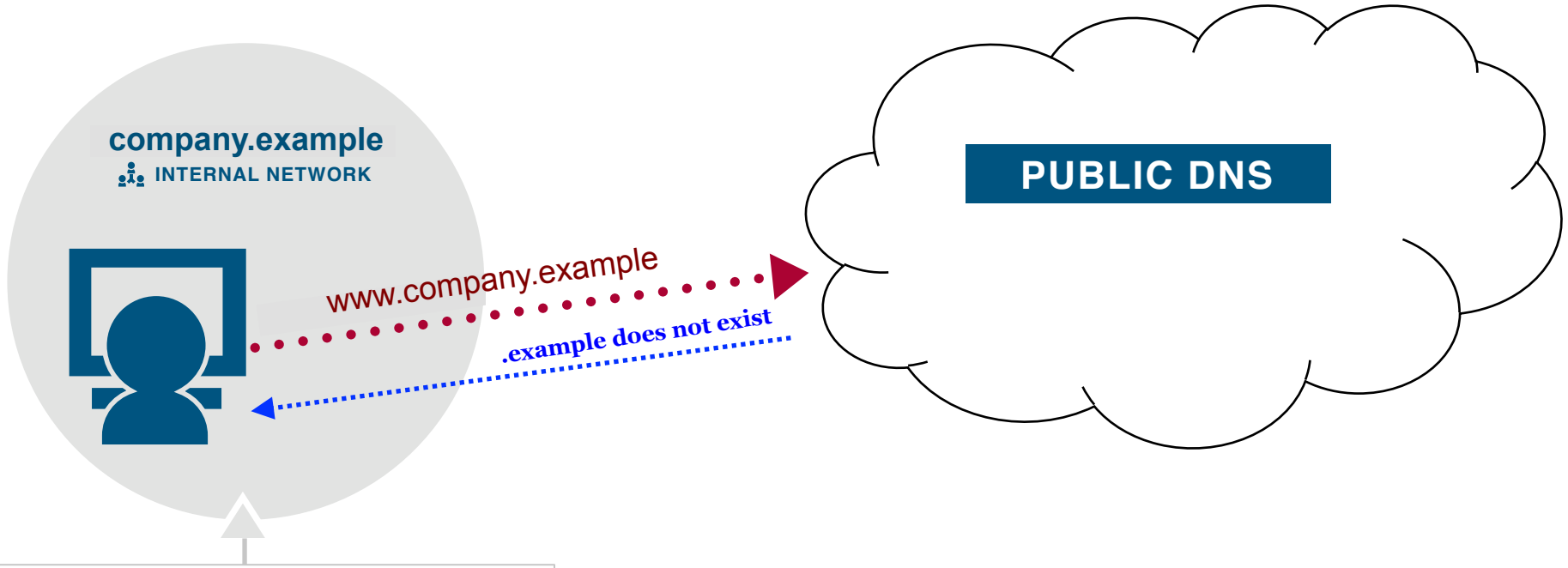
ICANN

Agenda

- Name Collisions
- Mitigation Measures in New gTLDs
- Where to Obtain Help
- Q&A

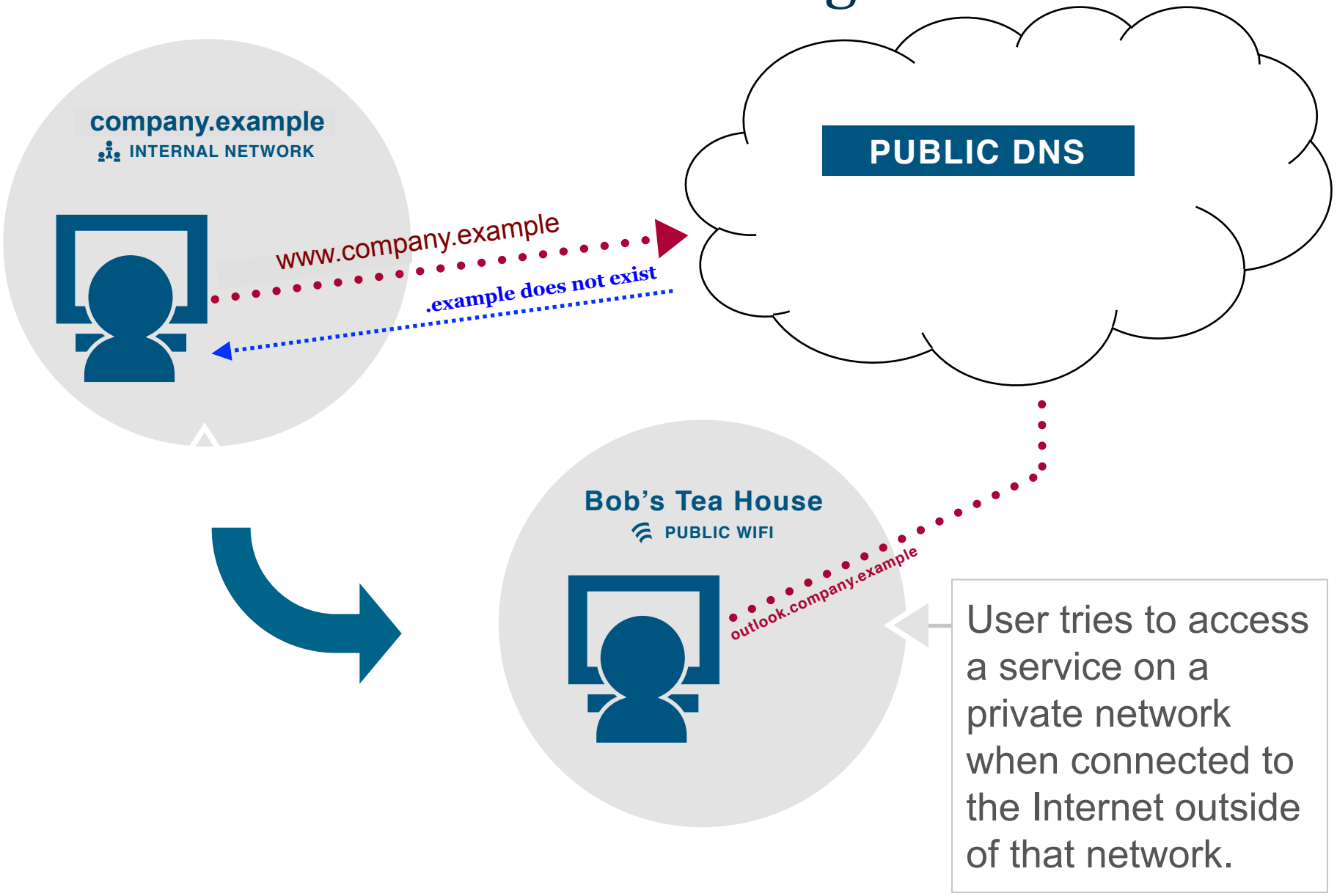
Name Collisions

Name Collision – The Leak



Private network configured in such a way that could “leak” the request to the public Domain Name System, when using a name in a private network that *does not exist* in the public DNS

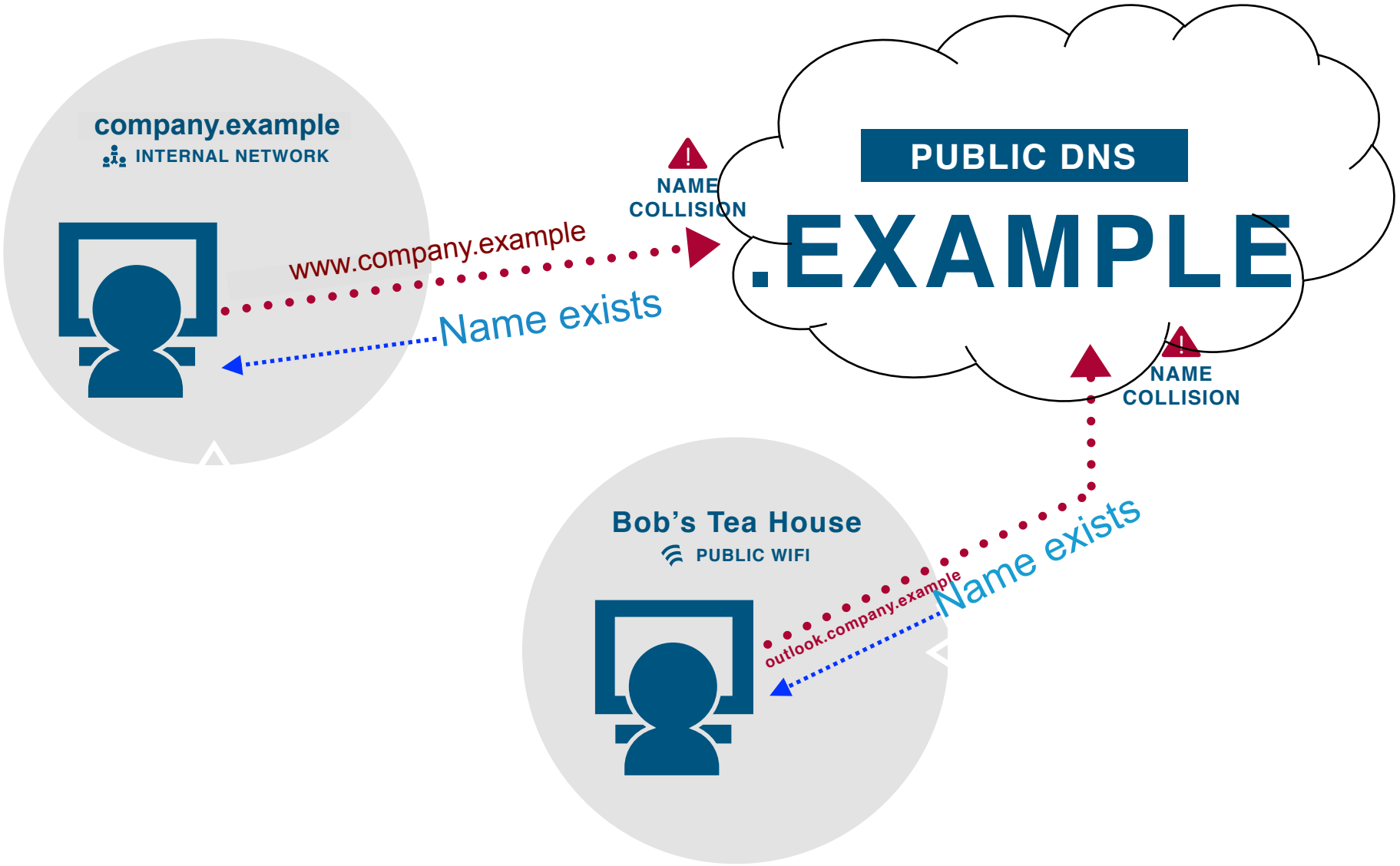
Name Collision – The Roaming Leak



Why Does This Happen?

- Local DNS Name spaces
  - Split-brain DNS
  - Use of “adopted” names, from documentation
- Search List Processing
  - Use of short unqualified domain names
  - Falling back on DNS lookup failure

Name Collision – The “Crunch”



As New Top-Level Domains are Added

- Once-failing names might “succeed”
  - The name to address result may be different
- Operational Interruption
  - At best, a nuisance to the user
  - At worst; data leakage, security breach, etc.

Mitigation Measures in New gTLDs

Mitigation Measures for New gTLDs

- Defer delegating three applied-for strings – high risk strings
- 120-day no activation of names from contract signing – internal name certificates mitigation
- Name collision reporting and emergency response – for those that have collisions
- 90-day Controlled Interruption (CI) after delegation of new gTLD – general notification

Controlled Interruption

- When a new generic top-level domain opens
  - A set of responses are returned for:
    - all names (wildcard TLD CI); or
    - a set of names that might be subjects of collision (SLD CI)
  - Designed to be a nuisance to those leaking queries
  - Designed to contain the damage of a data breach
- “Breadcrumbs” left in
  - Logs (of connection failures)
  - Intrusion Detection Systems (suspicious addressing)

127.0.53.53

- A “curious” loopback address
  - Meant to make connections fail, no data sent out
  - Meant to encourage operators to “look this up”
- Other clues that fixes are needed
  - Mail server is “**your-dns-needs-immediate-attention.<*tld*>**”
  - SRV lookup returns that same hostname
  - TXT record says “**Your DNS configuration needs immediate attention see https://icann.org/namecollision**”

Why no IPv6 address for CI?

- IPv4 has a /8 that has become dedicated to loopback
  - A waste, but, we have the space to play with
- IPv6 is more efficient, only a /128 for loopback
- What about IPv4 mapped addresses?
  - Lack of standardized implementation
  - Variations in OS treatment of those address
  - Use less predictable than desired

Flat SLD CI

- At first required “flat” SLD CI:

```
<label>.<TLD>. 3600 IN A 127.0.53.53

<label>.<TLD>. 3600 IN MX 10 your-dns-needs-immediate-
attention.<TLD>.

<label>.<TLD>. 3600 IN SRV 10 10 0 your-dns-needs-immediate-
attention.<TLD>.

<label>.<TLD>. 3600 IN TXT "Your DNS configuration needs
immediate attention see https://icann.org/namecollision"
```

Wildcard SLD CI

- Now strongly recommend adding “Wildcard”:

```
*.<label>.<TLD>. 3600 IN A 127.0.53.53

*.<label>.<TLD>. 3600 IN MX 10 your-dns-needs-immediate-
attention.<label>.<TLD>.

*.<label>.<TLD>. 3600 IN SRV 10 10 0 your-dns-needs-
immediate-attention.<label>.<TLD>.

*.<label>.<TLD>. 3600 IN TXT "Your DNS configuration needs
immediate attention see https://icann.org/namecollision"
```

Current Status of CI

From ICANN CI monitoring:

- 344 TLDs in SLD CI
- 78 TLDs in Wildcard TLD CI
- 4 TLDs have not yet started CI

Web Ads Statistics

Campaign dates: 24 July – 28 Oct 2014

- Impressions: 6,322
- Clicks: 550
- Click through rate: 8.70%
- #1 keyword: 127.0.53.53

Reports of Harm

- Received 11 reports so far
  - 4 are search list related
  - 4 are internal name spaces.
  - 2 caused by configuration typo
  - 1 unknown
- No reports involve harm to human life

Where to Obtain Help

How to Avoid Name Collisions

- Use only Public-DNS, Fully Qualified Domain Names
- Avoid or limit reliance on search lists

Make sure to catch all the places where short, unqualified domain names have been used

Resources

- Guide to Name Collision Identification and Mitigation for IT Professionals
  - https://www.icann.org/en/system/files/files/name-collision-mitigation-01aug14-en.pdf
- If suffering name collision, report it to ICANN
  - https://forms.icann.org/en/help/name-collision/report-problems
- For further information, consult
  - https://icann.org/namecollision

Q&A

- Want to know “what’s coming”?
  - https://newgtlds.icann.org/newgtlds.csv
  - Includes name, contract date, delegation date

https://icann.org/namecollision

Social Media

https://twitter.com/ICANN

http://gplus.to/icann

https://www.facebook.com/icannorg

http://weibo.com/icannorg

http://www.linkedin.com/company/icann

ICANN