AI Trust & Governance With DNS

Nic Williams, nic@infoblox.com

Our Perspective

Discovery of Agents, Workloads, and Named entities

Problem

- AI agents, services, and tools increasingly interact without pre-existing relationships
- No structured interaction; do a search, use a URL and hope, OR hard code? Risks? Trust?

Discovery

- “Which entities exist that can perform a given function?”
- Discovery ≠ negotiation, execution, governance, or control

Discovery is foundational infrastructure:

- Enables interoperability
- Scales trust and safety mechanisms
- Keeps policy and control decoupled from core plumbing

Principles

- Treat agents, services, and tools uniformly as entities
- Keep discovery minimal, neutral, and composable
- Policy acts on top of discovery — not inside it

Takeaway

- No scalable, trustworthy AI ecosystem without a shared discovery layer

Deutsche Telekom

HUAWEI

NOKIA

Source: https://github.com/danielkinguk/discovery/blob/main/README.md#problem-statement-and-work-scope

Why DNS?

Practicality

- BGP glues together the networks making up the Internet, DNS facilitates everything communicating over it… these are the two "glue" protocols of the internet.
- Largest scale of deployed federated / decentralized protocols (~500T daily queries, ~10^104 total namespace permutations).
- Leverage existing technology expertise / employees: developers, vulnerability community, enterprises use and integrate to existing technologies to current network stack.
- Reduce internet fragmentation utilizing all the above to give AI workloads a known entry point to organizations using existing digital trust boundaries (domain + certificates a la DNSSEC, DANE, mTLS, etc.)… right now 😎.

Governance

- Root zone operation / control federated across borders.
- Diversity of hosting options across TLDs, registrars, registries, and even the hosting infrastructure.
- *Accepted universal domain takedown process (UDRP).*
- Increase individual operator sovereignty while decreasing third-party reliance: organizations advertise their own services without the risk of opaque registry rules or business practice (i.e. paid placement of less-reputable agents), delegate authority to business partnerships without need for registry approval.
- Organizations have sovereignty, the alternative might be commercial agent registries.

Why DNS?

Practicality

- BGP glues together the networks making up the Internet, DNS facilitates everything communicating over it… these are the two "glue" protocols of the internet.
- Largest scale of deployed federated / decentralized protocols (~500T daily queries, ~10^104 total namespace permutations).
- Leverage existing technology expertise / employees: developers, vulnerability community, enterprises use and integrate to existing technologies to current network stack.
- Reduce internet fragmentation utilizing all the above to give AI workloads a known entry point to organizations using existing digital trust boundaries (domain + certificates a la DNSSEC, DANE, mTLS, etc.)… right now 😎.

Governance

- Root zone operation / control federated across borders.
- Diversity of hosting options across TLDs, registrars, registries, and even the hosting infrastructure.
- *Accepted universal domain takedown process (UDRP).*
- Increase individual operator sovereignty while decreasing third-party reliance: organizations advertise their own services without the risk of opaque registry rules or business practice (i.e. paid placement of less-reputable agents), delegate authority to business partnerships without need for registry approval.
- Organizations have sovereignty, the alternative might be commercial agent registries.

www.example.com.

12 Root Server Operators

a.root-servers.net	US	**Verisign, Inc.**
b.root-servers.net	US	**University of Southern California**
c.root-servers.net	US	**Cogent Communications**
d.root-servers.net	US	**University of Maryland**
e.root-servers.net	US	**NASA (Ames Research Center)**
f.root-servers.net	US	**Internet Systems Consortium, Inc.**
g.root-servers.net	US	**US Department of Defense (NIC)**
h.root-servers.net	US	**US Army (Research Lab)**
i.root-servers.net	SE	**Netnod**
j.root-servers.net	US	**Verisign, Inc.**
k.root-servers.net	NL	**RIPE NCC**
l.root-servers.net	US	**ICANN**
m.root-servers.net	JP	**WIDE Project**

Source: https://www.iana.org/domains/root/servers

2017 root POPs worldwide, source: https://root-servers.org/

www.example.com.

Top Level Domains (~1,600 TLDs)

Standard: **.com, net, .org, .edu**

Country Code (ccTLD): **.uk, .cn, .fr, .de**

Country-specific: **.gmbh**

Location: **.africa, .paris, .eu**

Sponsored: **.mil, .gov**

New: **.shop, .tech**

Corporate: **.aws, .bmw**

Source: https://www.iana.org/domains/root/servers

www.example.com.

Second Level Domains (SLDs)

Registries maintain the database of SLDs within a TLD, and registrars sell domains to registrants.

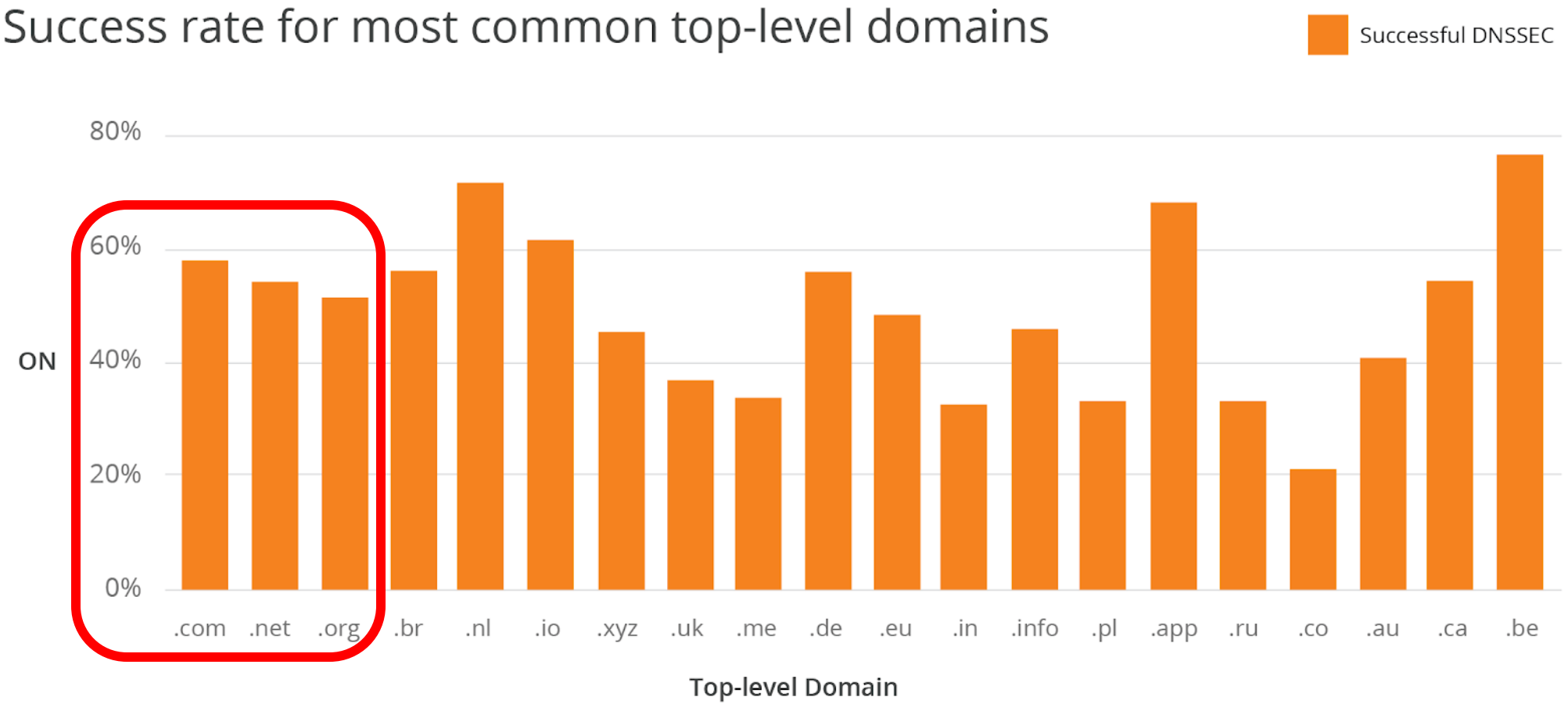
Sometimes effective SLDs for segmentation (i.e. .ac.uk versus .co.uk for education versus corporation).

All ~1,000 registries support a universal process for takedowns to enforce uniqueness, digital rights, and acceptable use.

www.example.com.

What parts of the existing domain governance/trust ecosystem should be extended to AI applications and workloads?

DNSSEC ("is this domain cryptographically anchored to the organization?")



Source: https://blog.cloudflare.com/automatically-provision-and-maintain-dnssec/

Additional DNS Trust Capabilities

Much more than just "what is the IP address?" ➡️ Public mechanisms to weigh trust and proof agents to organizations

Domain Control Verification (DCV)

Can the entity I'm talking to prove it represents the domain (organization)? "If you really are an agent of example.com, publish a TXT record with this hash."

DNS-based Authentication of Named Entities (DANE)

The domain owner publishes “this is the exact key/certificate you should see for this service”, and signs with DNSSEC. If the key doesn’t match, the connection is rejected. Example: email 📧.

Protective DNS (PDNS)

Governments, internet service providers (ISPs), and enterprises implement intelligence at the resolver to weigh domain reputation to build dynamic policy to inform trust decisions e.g. "this is a known good domain/agent, go ahead and communicate". Facilitates real-time blocking and retroactive analysis.

Zero Trust DNS (ZTDNS)

Enforces all endpoints within an organizational boundary do not egress without prior resolution through a trusted resolver.