SAC123: SSAC Report on the Evolution of Internet Name Resolution

Barry Leiba

ICANN79 DNSSEC & Security Workshop

6 March 2024

ICANN | SSAC

Security and Stability Advisory Committee

‘When I use a word,’ Humpty Dumpty said in rather a scornful tone, ‘it means just what I choose it to mean--neither more nor less.’

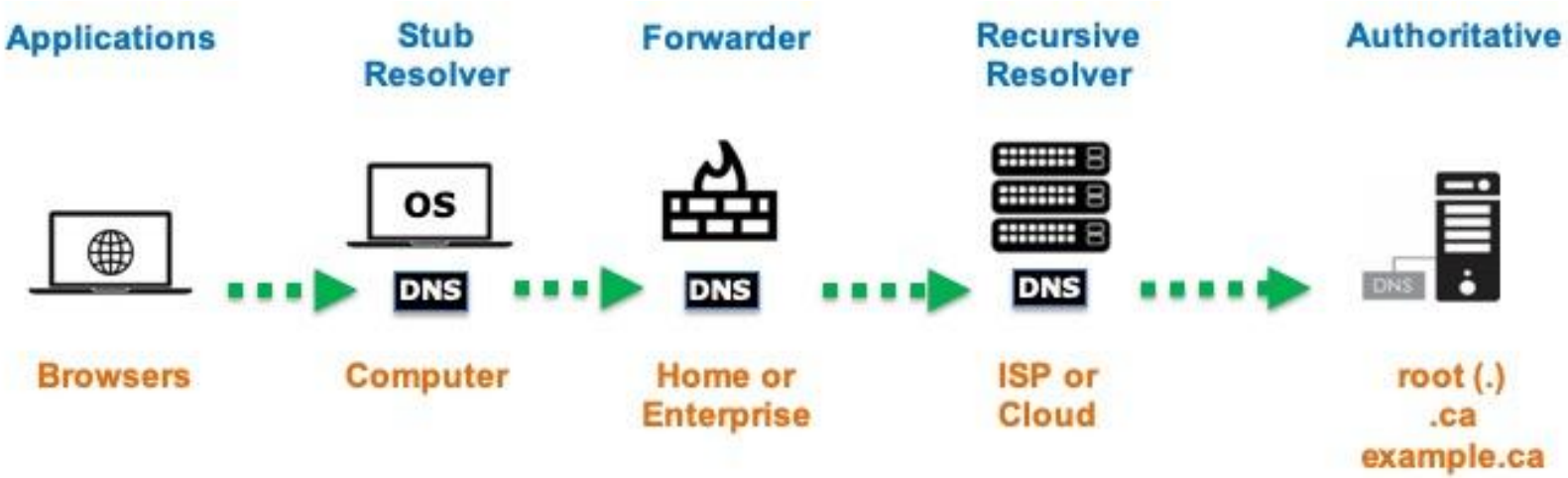
‘The question is,’ said Alice, ‘whether you CAN make words mean so many different things.’

Lewis Carroll, *Through the Looking-Glass and What Alice Found There*

Introduction

- Names play an important role in how users trust the services they use on the Internet
- Domain name resolution is becoming more ambiguous
- Names are becoming less visible, or at least less conspicuous, to users
- Evolving needs have spurred the development of alternative naming systems with varied principles and functionalities
- This report explores the effects and implications of alternative naming systems

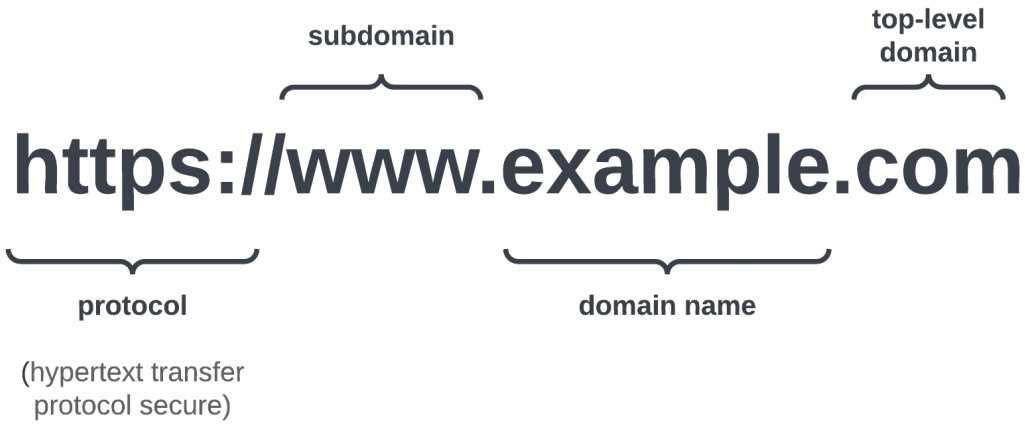
Traditional DNS Resolution



- DNS library is included in operating systems (OS)
- Library's operational parameters are usually automatically configured via Dynamic Host Configuration Protocol (DHCP)
- Applications rely on the OS's DNS library for name resolution, ensuring a unified method across different applications but reducing direct interaction with DNS settings

Domain Name Syntax

- A typical DNS domain name consists of a series of labels separated by dots ('.')
- Each label corresponds to a level in the DNS hierarchy



- **Motivations to Reuse Domain Name Syntax in Alternative Naming Systems**
  - ➜ **User Familiarity:** The consistent use of domain name syntax makes it easier for users to recognize and remember website addresses
  - ➜ **Compatibility Desire:** By adhering to DNS syntax, alternative naming systems can function alongside traditional DNS within their bundled applications

Motivations to Change Internet Name Resolution

The DNS was designed in the 1980s hierarchically within the technical constraints of that era, such as limited memory and processing power.

- ➜ Hierarchical structure facilitated ***delegated governance*** and an ***iterative name resolution process***

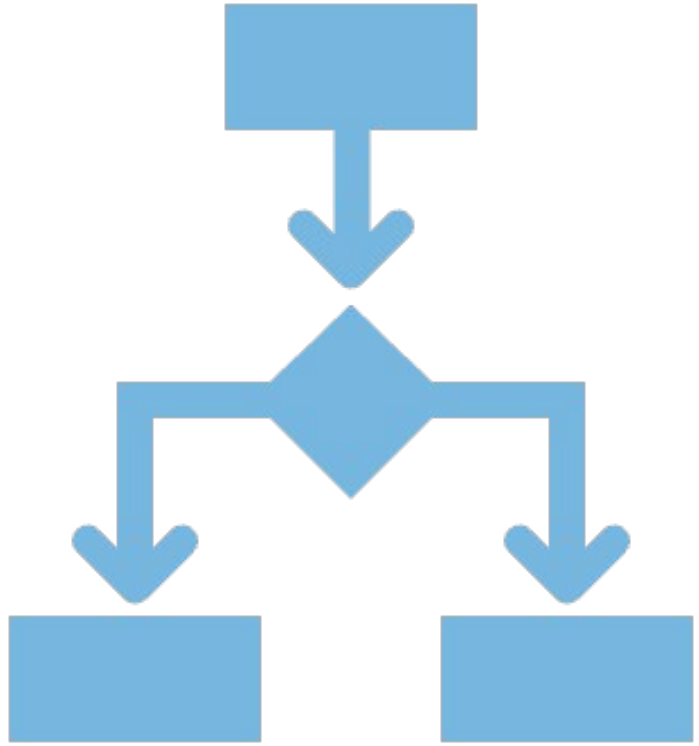
Motivations for Change:

- ➜ Speed Enhancements
- ➜ Privacy Concerns
- ➜ Authentication Enhancements
- ➜ Decentralized Governance
- ➜ Censorship Resistance

For an alternative system to gain wide acceptance, it needs to stand out in some fashion and provide functionality or overcome some technical limitation of the DNS.

Alternative Naming Systems in Use Today

- Many alt naming systems come bundled with specific applications which often bypasses administrator-controlled settings and any pre-configured DNS settings
  - ➜ Naming System: Tor
  - ➜ Application: Tor Browser
  - ➜ Context: The Tor Browser will use the Tor naming system for names ending in .ONION and the DNS for everything else
- The shift from a single, universally understood [DNS] resolution context to multiple, application-specific contexts requires users to understand the intended resolution protocol or trust the application to make the correct decision.
  - ➜ Ambiguity in Internet name resolution can give unexpected results and therefore ***undermines trust*** in the integrity of services on the Internet.



Examples of Alternative Naming Systems

Multicast DNS (.LOCAL)	• Local network resolution system using .LOCAL for device discovery without a central server • Does not use DNS protocol, not designed to interoperate with global DNS
Tor (.ONION)	• Provides anonymous service connections with non-memorable, hashed domain names • “vanity” .ONION domains can be created by users by repeatedly generating names until finding one that is memorable
Ethereum Name Service	• Based on Ethereum, a decentralized blockchain that allows the embedding of logic into its blocks to implement what are referred to as smart contracts • Maps readable, dot-separated labels names like "alice.eth" to Ethereum addresses, cryptocurrency wallet addresses, and InterPlanetary File System identifiers
Unstoppable Domains	• Reservation of second-level domain names in a select set of TLDs (.888, .BITCOIN, .BLOCKCHAIN, .COIN, .CRYPTO, .DAO, .NFT, .WALLET, .X, and .ZIL.) • Built on top of the Polygon blockchain platform • Maps names to cryptocurrency wallet addresses and InterPlanetary File System identifiers
Gnu Name System	• Decentralized replacement for DNS, integrating with the GNUnet framework using a distributed hash table • Allows users to register names as top-level domains (TLDs) and resolve other namespaces within their TLDs • There is no guarantee that names will be globally unique, or that a given name will resolve the same for different user

Trade-offs of Alternative Naming Systems

Naming System	Decentralized	Secure	Human Memorable
Multicast DNS (.LOCAL)	Moderate	Moderate	High
Tor (.ONION)	High	High	Low
Ethereum Name Service	High	Moderate	Moderate
Unstoppable Domains	Moderate	Moderate	High
Gnu Name System	High	High	Depends Names are either - LOW: global and not memorable, or - HIGH: not globally unique and memorable

Multicast DNS

Multicast DNS (.LOCAL)

Tor (.ONION)

Ethereum Name Service

Unstoppable Domains

Gnu Name System

Decentralization	Security	Human Memorability
• Operates in a peer-to-peer fashion • Devices announce their presence and services directly to others on the network. • Eliminates the need for a central server	• Reliance on multicast communication can introduce security vulnerabilities • Malicious actors could potentially spoof device identities or inject false information into the network	• Allows devices and services to advertise themselves using human-readable names

Tor (.ONION)

- Multicast DNS (.LOCAL)
- **Tor (.ONION)**
- Ethereum Name Service
- Unstoppable Domains
- Gnu Name System

Decentralization

- Operates on a distributed network of volunteer-run relays
- Eliminates any central authority
- Resistant to control or manipulation by any single entity

Security

- Prioritizes user anonymity and privacy by employing onion routing
- Encrypts data multiple times and routes it through a series of relays, making it difficult to track the origin or destination of the traffic

Human Memorability

- Tor does not utilize human-readable names for resources or services accessible within the network
- Relies on long, alphanumeric strings of characters that are difficult to remember or decipher

Ethereum Name Service

- Multicast DNS (.LOCAL)
- Tor (.ONION)
- **Ethereum Name Service**
- Unstoppable Domains
- Gnu Name System

Decentralization	Security	Human Memorability
• Operates on the Ethereum blockchain, a distributed ledger technology with no single point of control	• Leverages the security features of the Ethereum blockchain, including immutability and cryptographic verification	• Allows users to register names that are similar to traditional domain names

Unstoppable Domains

- Multicast DNS (.LOCAL)
- Tor (.ONION)
- Ethereum Name Service
- **Unstoppable Domains**
- Gnu Name System

Decentralization	Security	Human Memorability
• Leverages Polygon blockchain technology for name registration • Operates with a central authority managing the root domain and core infrastructure	• Leverages the security features of the Polygon blockchain, including immutability and cryptographic verification	• Allows users to register names that are similar to traditional domain names

Gnu Name System

- Multicast DNS (.LOCAL)
- Tor (.ONION)
- Ethereum Name Service
- Unstoppable Domains
- **Gnu Name System**

Decentralization

- Operates on a fully decentralized peer-to-peer network
- Eliminates any central authority or reliance on external servers

Security

- Employs strong encryption mechanisms and anonymity features to protect user identities and communication channels

Human Memorability

- Does not support names that are simultaneously global, secure, and memorable
- Global and not memorable: offers globally unique names for resources, but these names are cryptographic hashes, not human-readable words or phrases
- Not globally unique and memorable: Users can configure local, memorable "petnames" for specific zones, but these names are not globally unique and only work within the user's local configuration

Trends Impacting Trust and Security

Context

- ➜ Traditionally, internet naming has relied on ***referential integrity***, meaning regardless of who looks up a name, the response should consistently be what the domain administrator intended

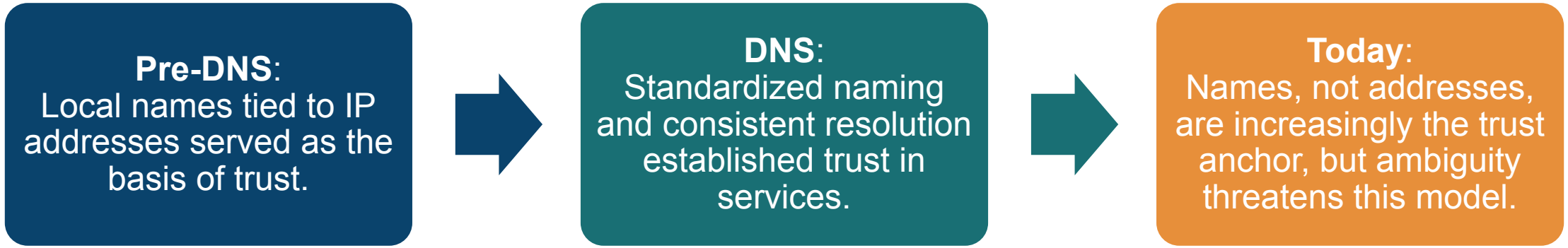
Emerging Trends Disrupting Referential Integrity

- ➜ Query-based resolution: This approach incorporates additional data (like user location) into the query, potentially leading to different responses for the same name depending on the context.
  - Example: "ECS (EDNS client-subnet)" tailors responses based on the querying client's location, impacting the resolved resources.
- ➜ The rise of alternative naming systems utilizing similar syntax creates confusion and potential conflicts.

Impact

- ➜ Users can no longer be sure of the context and outcome of resolving a name, potentially undermining trust and security
- ➜ This ambiguity creates opportunities for misuse, where malicious actors could exploit the confusion to deceive users or redirect them to unintended destinations

Implications of Ambiguous Internet Name Resolution



- ➜ The same name can resolve differently, leading to confusion and potential encounters with malicious actors masquerading as legitimate entities (e.g., phishing)
- ➜ Users encountering resolution errors due to namespace ambiguity lack the understanding to address the problem
- ➜ Technologies like QR codes obscure domain names, hindering users' ability to identify the true destination of a link

The combination of ambiguous resolution and reduced name visibility significantly undermines user confidence and trust in online services

Proposals to Facilitate Namespace Coordination

.INTERNAL

- SAC113
- Proposes reserving a portion of the namespace for private, internal DNS uses.

.ALT

- RFC 9476
- Proposes the .alt top-level domain for alternative naming systems

➜ Both proposals are ***voluntary*** and ***non-intrusive***

➜ They do not enforce usage but encourage good practices to ***minimize ambiguity***

➜ Widespread adoption could significantly mitigate namespace ambiguity and ***enhance online trust***

SSAC Recommendations

ICANN should **track and provide regular updates** on:

1. Alternative protocols that make use of the domain namespace, and
2. Efforts to create mitigations and reduce risks inherent in the coexistence of multiple namespaces and protocols.

ICANN should keep the ICANN community abreast of new developments through such means as the Emerging Identifier Technologies panels.

Discussion