ICANN 79 | COMMUNITY FORUM

Joint Session
SSAC and ALAC

Agenda

- Welcome and Opening Comments — Jonathan Zuck, Ram Mohan — 5 minutes

- Safer Cyber Campaign — Ram Mohan — 25 minutes

- Follow up on Urgent Requests — Steve Crocker — 10 minutes

- Implications for end-users on the Proposed Top-Level Domain for Private Use — Warren Kumari — 15 minutes

- Briefing on SAC123: SSAC Report on the Evolution of Internet Name Resolution — Barry Leiba — 15 minutes

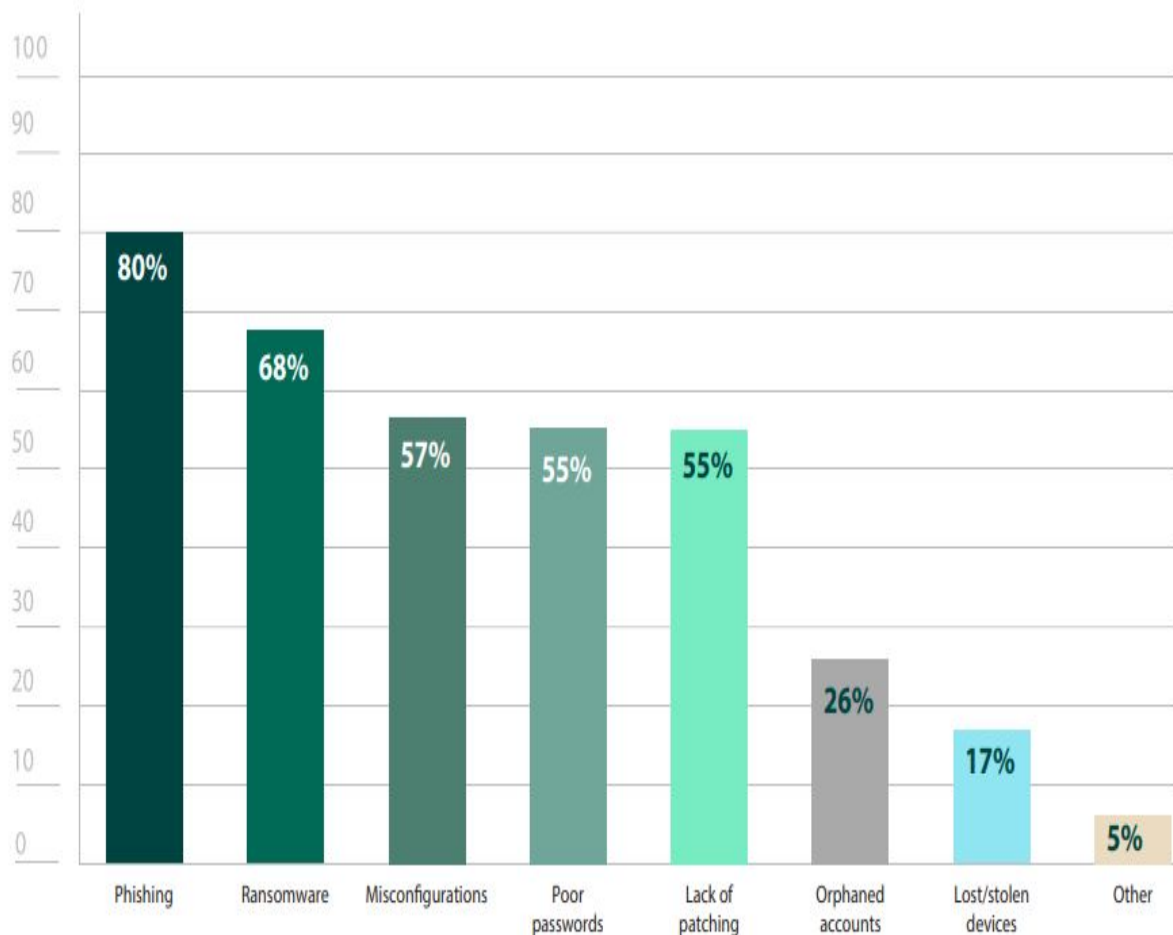- Closing Comments and Next Steps — Jonathan Zuck, Ram Mohan — 5 minutes

Safer Cyber Campaign

Ram Mohan

Cybersecurity Is Infrastructure
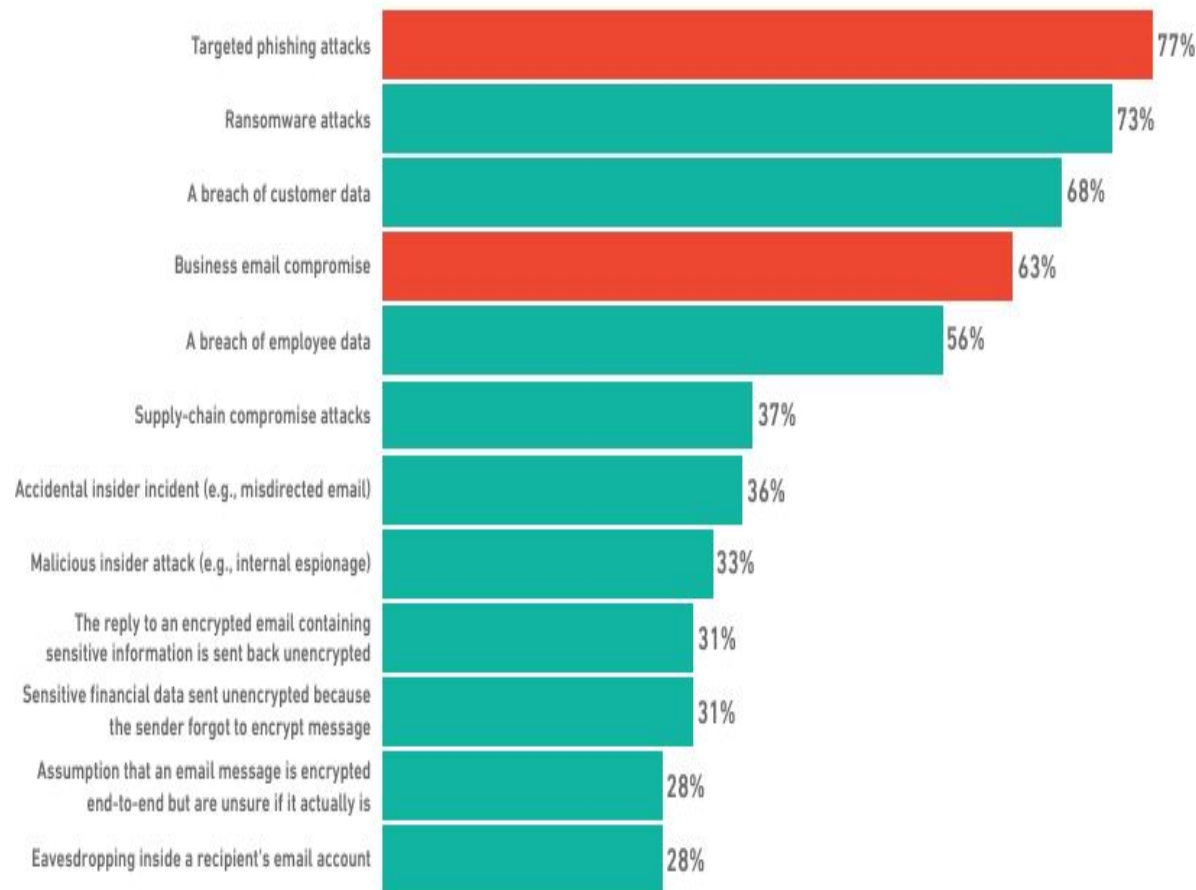

Common Security Concerns

What common security risks/entry points are you most concerned about?

Phishing	80%
Ransomware	68%
Misconfigurations	57%
Poor passwords	55%
Lack of patching	55%
Orphaned accounts	26%
Lost/stolen devices	17%
Other	5%

https://terranovasecurity.com/wp-content/uploads/2022/12/phishing-stats.png

Level of Concern About Types of Cyberattacks

Percentage of respondents indicating "concerned" or "extremely concerned"

Targeted phishing attacks	77%
Ransomware attacks	73%
A breach of customer data	68%
Business email compromise	63%
A breach of employee data	56%
Supply-chain compromise attacks	37%
Accidental insider incident (e.g., misdirected email)	36%
Malicious insider attack (e.g., internal espionage)	33%
The reply to an encrypted email containing sensitive information is sent back unencrypted	31%
Sensitive financial data sent unencrypted because the sender forgot to encrypt message	31%
Assumption that an email message is encrypted end-to-end but are unsure if it actually is	28%
Eavesdropping inside a recipient's email account	28%

"How to Deal with Business Email Compromise," Osterman Research, Sponsored by SonicWall, January 2022

https://www.sonicwall.com/medialibrary/en/white-paper/2022-sonicwall-cyber-threat-report.pdf

Discussion Questions on Safer Cyber Campaign

- **Shared values:** keep the DNS secure and stable for end users

- **Opportunity:** how can SSAC and ALAC effectively collaborate to reach diverse audiences?

- **Focus:** curate and disseminate the most impactful DNS security information

- **Considerations**:

  ➔ who are the primary and secondary audiences we should prioritize?

  ➔ what combination of informational campaign methods would be most effective in each region?

  ➔ regional contexts to consider?

Urgent Requests for Disclosure of Registration Data

Steve Crocker

Key Findings from SAC122

- **Key SSAC Concerns**
  - Lack of specific submission mechanism for Urgent Requests; reliance on general Disclosure Request process.
  - Response times "generally" within 24 hours, extendable up to 7 days, deemed insufficient for situations described as posing an "imminent threat to life" or serious harm.

- **The SSAC examined four aspects of the policy to determine it was not fit-for-purpose:**
  - **Fitness:** Current policy may not adequately address urgent needs for rapid disclosure.
  - **Transparency:** Ambiguities in policy terms and rationale; clarity needed.
  - **Reputation:** Potential negative impact on ICANN's image regarding responsiveness to critical situations.
  - **Process:** Challenges in the existing process in effectively addressing urgent disclosure requests.

- SSAC notes the language for urgent requests has been removed from the Registration Data Policy published on 21 February 2024

SAC122 Recommendations

Recommendation 1: The policy must provide additional structure so that Urgent Requests will be handled in an appropriately expedited fashion.

Recommendation 2: The policy must ensure that response times for handling Urgent Requests be fit for purpose.

Recommendation 3: ICANN org should acquire and document data regarding Urgent Requests and make high-level information available to the community for future consideration.

Implications for end-users on the Proposed Top-Level Domain for Private Use

Warren Kumari

Some background…

- Started off in the IETF (2017) as [draft-wkumari-dnsop-internal - "The .internal TLD."](#)
  - DNSOP participants (rightly) observed that this should be done in ICANN

- Brought to ICANN SSAC, and became [SAC113: SSAC Advisory on Private-Use TLDs](#)

SAC113: SSAC Advisory on Private-Use TLDs

- Report contains a number of "Use-Cases for Private-Use TLDs", but one obvious justification is that people keep doing this (e.g .home, .corp, .mail, .internal)

Magnitude ▼	Top-Level Domain ▲▼
8.128	internal
8.018	localdomain
7.807	lan
7.778	olk
7.600	home
7.431	unifi
7.290	initplayback
7.194	wpad
7.143	server
7.141	corp
7.014	https

Source: https://magnitude.research.icann.org/

Magnitude ▾	Top-Level Domain ▲▾	status ▲▾	Daily Rank ▲▾	Weekly Rank ▲▾	Monthly Rank ▲▾	Quarterly Rank ▲▾	Coverage ▲▾	Unique Sources ▲▾	Queries Per Thousand ▲▾	Query Volume ▲▾	Avg Query/Source ▲▾
8.128	internal		▼ 46	▲ 43	▲ 45	46	7%	82,144	6%	26,028,235	316
8.018	localdomain		▼ 59	55	▼ 55	54	6%	70,556	3%	14,356,260	203
7.807	lan		▼ 91	▲ 90	▲ 92	97	4%	52,541	13%	54,807,233	1,043
7.778	olk		▲ 99	▲ 141	▲ 143	159	4%	50,490	0%	1,184,746	23
7.600	home		▼ 127	▲ 124	136	136	3%	39,387	23%	98,851,218	2,509
7.431	unifi		▼ 178	▲ 160	▲ 188	198	2%	31,150	2%	8,336,745	267
7.290	initplayback		▲ 231	▲ 233	▲ 254	260	2%	25,586	0%	1,216,699	47
7.194	wpad		259	▲ 259	▲ 275	278	2%	22,405	0%	1,005,932	44
7.143	server		▼ 285	▲ 279	293	293	1%	20,845	0%	1,010,302	48
7.141	corp		▲ 287	▲ 296	▲ 301	302	1%	20,807	9%	39,014,423	1,875
7.014	https		▼ 323	▲ 320	324	324	1%	17,426	0%	600,410	34
6.971	null		▼ 334	▼ 332	331	331	1%	16,416	0%	1,620,590	98
6.954	tcs		▲ 338	▼ 351	▼ 347	346	1%	16,030	0%	287,830	17
6.924	bind		▼ 348	▲ 338	▼ 341	340	1%	15,366	1%	5,452,724	354
6.895	loc		▼ 355	▲ 353	▲ 359	365	1%	14,768	3%	14,641,075	991
6.836	workgroup		▲ 376	▼ 391	▼ 384	376	1%	13,607	0%	1,740,650	127
6.829	undefined		▼ 377	▲ 376	▲ 379	393	1%	13,475	0%	892,047	66
6.816	lp-prun-web		▲ 380	▲ 390	392	392	1%	13,223	0%	233,876	17
6.763	comgeforce		▼ 396	▲ 392	▼ 400	399	1%	12,281	0%	269,101	21
6.755	comhttps		▲ 398	▼ 410	▼ 394	385	1%	12,155	0%	812,969	66
6.755	intra		▲ 399	▲ 416	▲ 427	434	1%	12,149	3%	15,960,465	1,313
6.754	mi		▲ 400	▲ 425	▲ 485	535	1%	12,131	0%	310,486	25
6.732	dummy		▼ 407	▲ 400	▲ 407	408	1%	11,763	0%	660,493	56
6.731	citrix		▲ 408	▼ 505	▲ 494	503	1%	11,757	0%	171,913	14
6.713	adsl		▲ 416	▼ 440	▼ 428	425	1%	11,465	0%	100,870	8
6.704	dlink		▲ 421	▲ 428	▲ 443	455	1%	11,325	1%	4,997,149	441
6.700	event		▼ 424	▲ 418	▼ 424	422	1%	11,258	0%	311,990	27
6.700	comxh-shared		▼ 425	▲ 420	▲ 425	–	1%	11,248	0%	788,384	70
6.697	col		▼ 428	▲ 415	420	420	1%	11,203	0%	1,386,941	123
6.692	tld		▼ 431	▼ 422	▲ 414	415	0%	11,132	0%	1,401,438	125
6.688	autodesk		▲ 433	▲ 511	▼ 532	558	0%	11,066	0%	139,157	12
6.662	srv		▼ 444	▼ 430	▼ 429	421	0%	10,671	0%	902,213	84
6.627	http		▼ 458	450	▼ 450	443	0%	10,174	0%	608,265	59
6.620	fe80		▼ 460	▲ 437	▲ 452	457	0%	10,068	0%	235,969	23
6.614	eu11		▲ 462	▼ 472	▼ 461	429	0%	9,989	0%	251,291	25
6.606	com11		▲ 465	▼ 482	▼ 464	430	0%	9,873	0%	262,979	26
6.605	intranet		▲ 467	▲ 469	▲ 474	476	0%	9,864	2%	11,884,349	1,204
6.604	cn11		▲ 470	▼ 480	▼ 466	431	0%	9,846	0%	234,082	23
6.599	asia11		▲ 474	▼ 483	▼ 468	435	0%	9,781	0%	221,976	22
6.591	txt		▼ 478	▲ 451	▲ 473	481	0%	9,668	0%	549,196	56
6.581	lgwebostv		▼ 481	▲ 466	▲ 515	536	0%	9,531	0%	550,661	57
6.556	api		▼ 490	▼ 486	▼ 484	477	0%	9,205	0%	707,478	76
6.547	js		▲ 495	▼ 510	▼ 481	471	0%	9,097	3%	14,165,630	1,557
6.530	intern		▲ 503	▲ 526	▲ 590	620	0%	8,877	0%	1,730,989	194

ICANN|SSAC

SAC113: SSAC Advisory on Private-Use TLDs

The SSAC recommends that the ICANN Board ensure a string
is identified using the criteria specified in Section 4.1
and reserved at the top level for private use.

This particular string must never be delegated.

The SSAC proposes the following criteria for the selection of the string:

1. It is a valid DNS label
2. It is not already delegated in the root zone.
3. It is not confusingly similar to another TLD in existence.
4. It is relatively short, memorable, and meaningful.

Public Comment

Proposed Top-Level Domain String for Private Use

The Internet Assigned Numbers Authority (IANA) has made a provisional determination that ".INTERNAL" should be reserved for private-use and internal network applications. Prior to review and approval of this reservation by the ICANN Board, we are seeking feedback on whether the selection complies with the specified procedure from SAC113, and any other observations that this string would be an inappropriate selection for this purpose.

Implications for end-users

- Potential Benefits:
  - ☑ Improved security through clear differentiation between public and private namespaces
  - ☑ Reduced risk of name collisions with potential gTLDs, enhancing user trust and reliability in navigating the Internet
- Potential Challenges (Potential):
  - ⚠ Users may not be aware of ".INTERNAL" or readily adopt it, leading to potential confusion or continued use of non-designated domains
- SSAC and ALAC's Role

  SSAC: Providing technical expertise and guidance on the implementation and security implications.

  ALAC: Advocating for end-user interests, focusing on usability, accessibility, and awareness.

The Evolving Internet Name Resolution Space

Barry Leiba

SAC123: SSAC Report on the Evolution of Internet Name Resolution

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
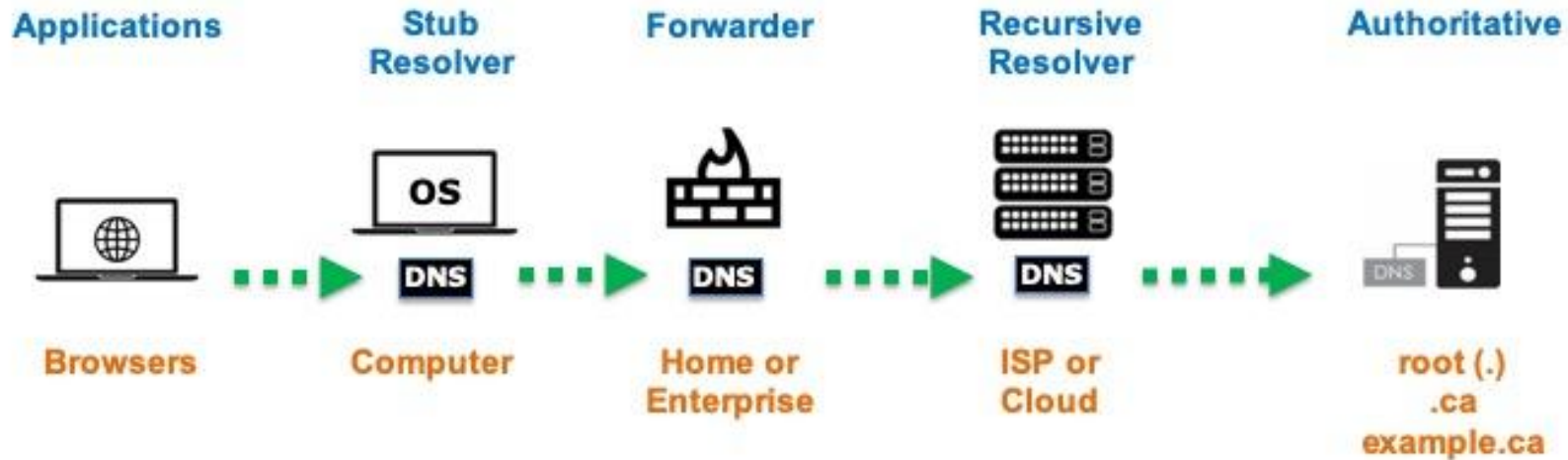
- DNS library is included in operating systems (OS)

- 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

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.
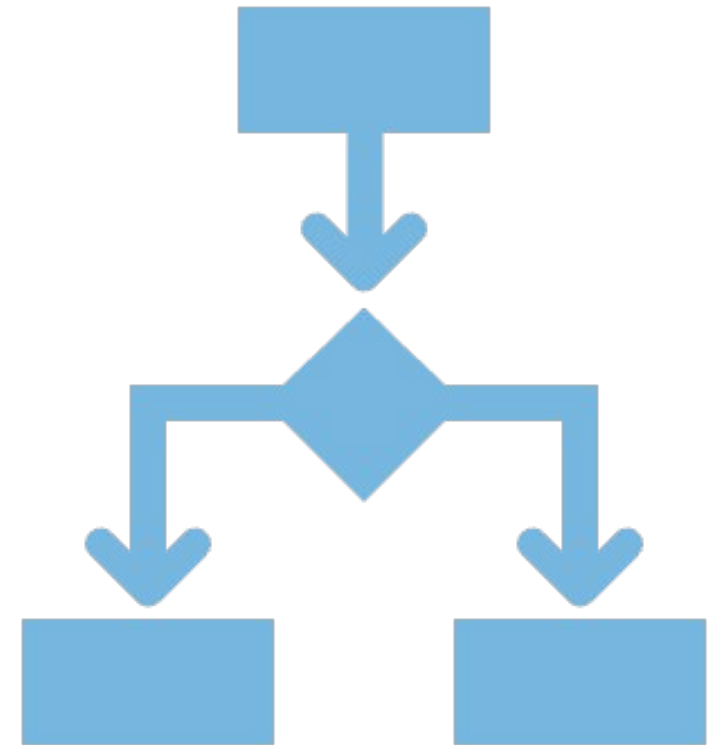
Examples of Alternative Naming Systems

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
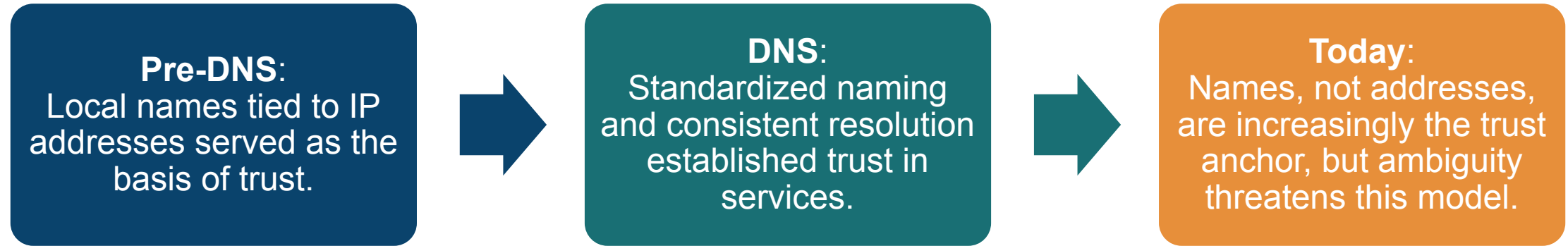
Gnu Name System
- Decentralized replacement for DNS, integrating with the GNUnet framework using a distributed hash table
- Allows users to register names as top-level domains (TLDs) and resolve other namespaces within their TLDs
- There is no guarantee that names will be globally unique, or that a given 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

Implications of Ambiguous Internet Name Resolution

Pre-DNS:
Local names tied to IP addresses served as the basis of trust.

→

DNS:
Standardized naming and consistent resolution established trust in services.

→

Today:
Names, not addresses, are increasingly the trust anchor, but ambiguity threatens this model.

- 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.

Next Steps

Jonathan Zuck and Ram Mohan

Come to the New SSAC Open Forum

➔ **Informal, drop-in-style session**

➔ **Opportunity to connect directly with SSAC members**

➔ **Get insights into the committee's current projects and initiatives.**

➔ **Ask questions about becoming a member and contributing to the SSAC's mission.**

➔ **Have questions about other SSAC sessions held throughout the week? This is your chance to get them answered**

➔ *Thursday, Block 1, Room 103 B*

ICANN|SSAC