ICANN 79 COMMUNITY FORUM

Inside IROS:
Identifier Research, Operations, and Security Function

Who We Are & What We Do

IROS

The IROS function
an umbrella that covers two teams:

Office of the Chief Technology Officer (OCTO)

Collecting data, researching and writing papers, providing training and capacity building, and trying to help identify and measure DNS security threats and abuse.

IANA Functions

Delivering the names, numbers, and protocol parameters functions that the community depends upon for the Internet to work.

OCTO functions in a nutshell

- **Operations**: Liaise between OCTO and other ICANN functional teams and facilitate OCTO-specific meetings and activities - ICANN DNS Symposium (IDS), Registry Operators Workshop (ROW), How it Works Workshops (HiW), as well as provide project management support to OCTO and IANA (as requested).

- **Technical Engagement (TE)**: Develop framework for organizations to cooperate, coordinate, and collaborate with ICANN on technical matters. Ensure a coherent technical engagement across ICANN by framing and communicating the organization's technical position.

- **Security Stability and Resiliency (SSR) Research**: Leads cybersecurity discussions and contributes subject matter expertise, research and tooling that, in one form or another, helps to maintain secure and resilient identifier systems.

- **Research**: Provide trusted and verifiable information to the Internet community regarding the system of unique identifiers. Perform studies or analyze data to better understand the health and well-being of the DNS ecosystem.

Technical Engagement

Adiel Akplogan - VP, Technical Engagement

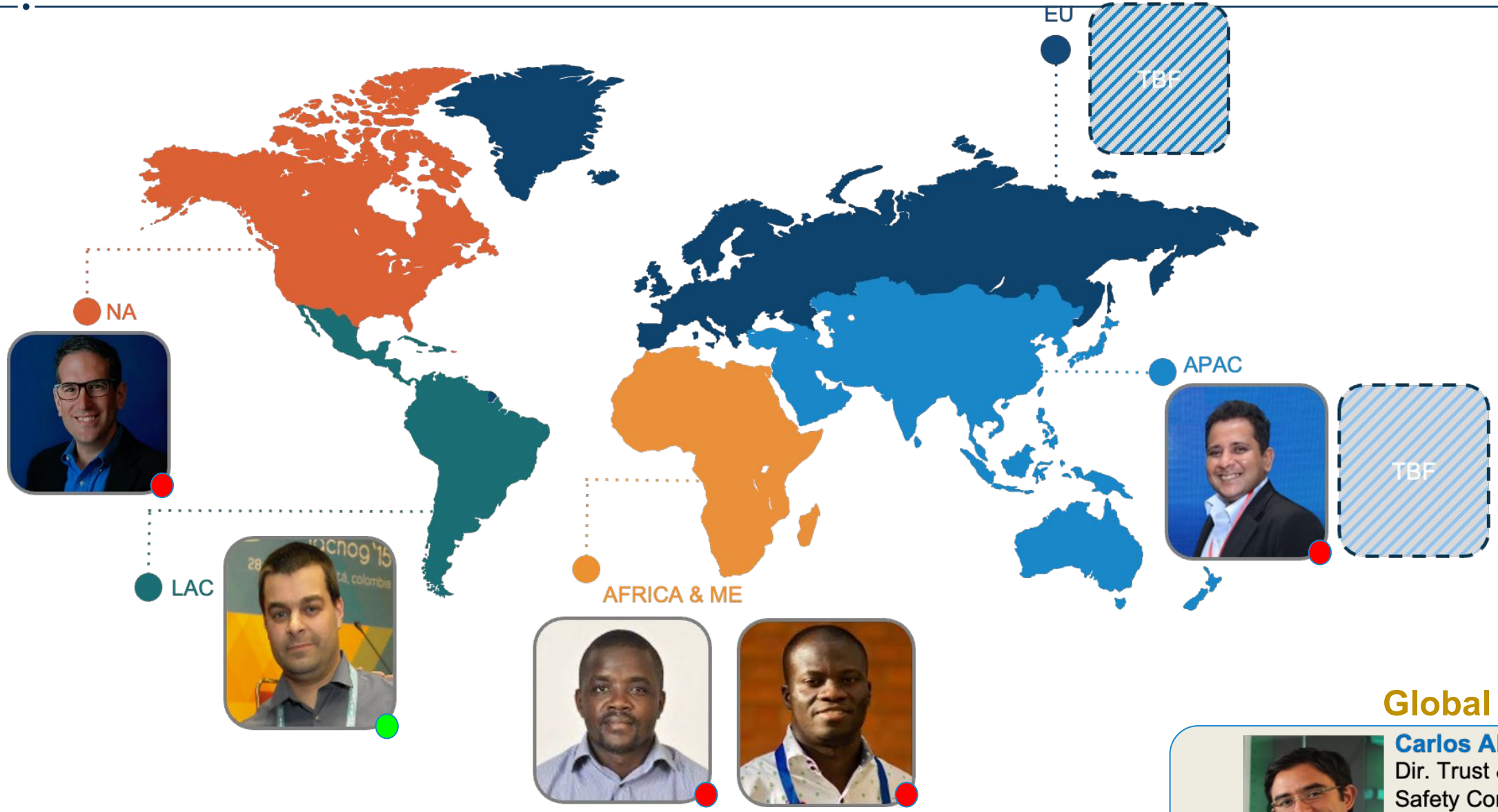
Technical Engagement in a nutshell

- Develop and sustain relationships with other technical organizations who share the vision and responsibility for secure, stable, and resilient unique identifier system coordination.
    - *Involve building a proper framework for organizations to cooperate, coordinate, and collaborate with ICANN on technical matters.*
- Coordinate ICANN the Knowledge-Sharing and Instantiating Norms for DNS and Naming Security (KINDNS - kindns.org) initiative.
- Lead and coordinate global ICANN's technical engagement programs.

Two Tracks for Technical Engagement

- Technical capacity building and outreach:
  - Regional/local training and capacity development programs
  - Technical content for online training platform (ICANN-Learn)
  - Training partnerships
- Engagement with the technical community:
  - Engagement with Law Enforcement and Public Safety Community
  - Promote ICANN's technical initiatives at technical events
  - Technical assessment of policies, regulations, and technology trends
  - Support regional communities on technical topics (IDNs, DNS, DNSSEC, security best practices for Internet Identifiers System)
  - Support SSAC, RSSAC, UASG, and other advising constituencies engagement efforts
  - Support CDA technical Tracks (DNSSEC Roadshow, IXP, IMRS & ccTLD Capacity Building)

TE Regional Coverage



Global

Carlos Alvarez
Dir. Trust & Public Safety Community Engagement

Technical Engagement

Security, Stability, & Resiliency Research

Dr. Samaneh Tajalizadehkhoob, Director SSR Research

SSR Research Goals

Support ICANN's contractual and operational commitment to ensure the security, stability, and resiliency of the topmost levels of the Internet's system of unique identifiers by:

- Understanding the state-of-the-art research
- Educating the community on the topics related to SSR of DNS
- Leading and carrying out research in the areas that is relevant to the SSR of DNS
- Creating tools, visuals and data that helps the community to understand and measure events related to SSR of DNS
- Facilitating cyber security discussions
- Contributing subject matter expertise or data that helps maintain secure and resilient identifier systems

Key SSR Research Activities

- Continuation of the Domain Abuse Activity Reporting (DAAR) system - Keep an eye for the updates on this in the Techday session at ICANN79
- Domain Name Security Threat Information Collection & Reporting (DNSTICR)
- Quantifying the prevalence and implications of "**Active**" Domains
  - Paper accepted and presented at IEEE Security & Privacy EUROPE 2023
- Developing a **classifier** for **unsolicited** email, based on data from APWG
  - Paper accepted and will be presented at TRUSTCOM 2023
- Developing Metrics that allows for Reputation Block Lists **Evaluations**
  - Paper accepted and presented at APWG e-crime 2023 conference
- Blockchain based domains based on **root data observations**
  - Initial research results presented at IDS 2023
- **DNS Abuse prediction** research
  - Flag potentially malicious domain names using ML techs
- Estimating malicious domains' **uptime**

Research

Matt Larson, VP, Research

Research Goals

- Provide trusted and verifiable information to the Internet community regarding the system of unique identifiers
- Engage actively with the DNS technology communities to identify issues that fall within ICANN's remit and will benefit from the focused attention our researchers can bring to bear on the issue
- Facilitate or participate with these same communities in preparedness activities to protect against or mitigate threats to DNS ecosystem
- Perform studies or analyze data to better understand the health and well-being of the DNS ecosystem
- Root server traffic research
- Facilitate the Name Collision Assessment Project (NCAP)
- Represent ICANN org on RSSAC

Research Activities

- Identifier Technology Health Indicators (ITHI)
  - Develop metrics to measure the health of the Internet's unique identifier system
- DNS authoritative servers and resolvers
  - Concentration and distribution
- Resource Public Key Infrastructure (RPKI)
  - Coverage of DNS servers and resolvers by Route Origin Authorizations (ROAs)
- DNSSEC error reporting
  - Develop protocol and facilitate and encourage implementation
- Published DNS top-level data sets
  - DNS Core (mapping the boundary between public and private DNS)
  - TLD apex history (TLD DNS metadata tracked over time)
- ICANN Managed Root Server (IMRS) behavior
  - Tracking round trip times from various locations

OCTO Document Series

- OCTO publishes technical documents written by OCTO authors in the OCTO document series
  - Series started in 2019
  - Published 38 documents and counting
- Recent examples:
  - Methodology to Classify Unsolicited Email Threats (OCTO-038)
  - RBL Evaluation Methodology (OCTO-037)
  - Round-Trip Times Between Resolvers and IMRS (OCTO-036)
  - Observing DNSSEC Key Lifecycles (OCTO-035)
  - Challenges with Alternative Name Systems (OCTO-034)
  - DNSSEC Algorithm Use in 2022 (OCTO-033)
  - DNS Resolvers Used in the EU (OCTO-032)
  - Quantum Computing and the DNS (OCTO-031)
- Links to all documents at https://www.icann.org/octo/publications

The work of the OCTO team

Where can you find it?

External work of the OCTO team

ICANN Blog

ICANN Publishes DNS Abuse Trends

22 March 2022

By Samaneh Tajaliz

DNS abuse is one of
is the right place to
mean by DNS abuse
coordinator of the D
program focused or

ICANN's 2021 LAC Engagement Sessions Reached Over 3,000 Stakeholders

22 December 2021

By Nicolás Antoniello and Daniel Fink

ICANN Publishes Paper on How Quantum Computing Will Affect the DNS in the Future

17 February 2022

By Paul Hoffman

The topic of quantum computing has appeared more often in the past few years because more people are concerned about its possible effects on security and privacy. If someone can build a very large quantum computer, it would completely undermine the cryptography that is used in digital signatures (such as those used in DNSSEC) and key exchanges for privacy (such as those used in TLS).

Speaking engagements