ICANN 69
VIRTUAL ANNUAL GENERAL

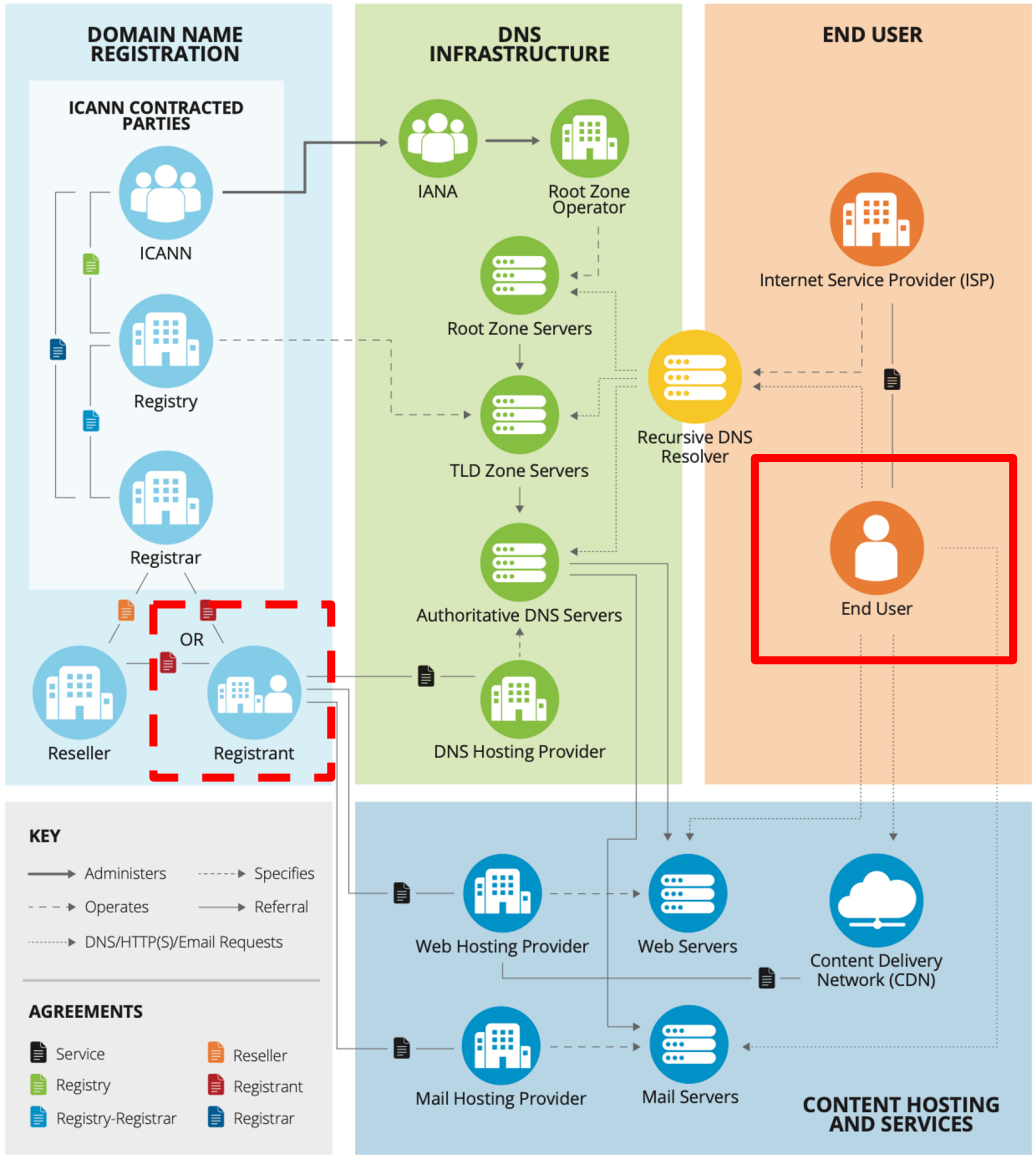
# The interests of the Internet end users as they relate to the security and stability of the Internet

Dr. Steve Crocker | ICANN69 | October 19, 2020

# Dr. Steve Crocker

- Internet Pioneer, early leader of ISOC and IETF
- Creator of RFC Series
- Chair of ICANN Security and Stability Advisory Committee (2003-2010)
- Chair of ICANN Board (2011-2017)

# DNS Ecosystem




To access internet resources in a secure and stable manner, internet end users rely on ISPs and the following stakeholders:

- Domain Name Registration
- DNS Infrastructure
- Content Hosting and services

# Conceptual Framework For Security

# Security Conceptual Framework

**CIA "Triad" - A security model that helps people think about various parts of IT security**

**Availability**: Ensuring data and services are available for use whenever required by their end users

**Integrity**: Maintaining the consistency, accuracy, and trustworthiness of data

**Confidentiality**: Preventing the disclosure of information to the wrong people while being used or stored by authorized end users

# Internet and Users: Availability

- Ensuring the baseline
  - "Root" DNS provides the foundation of the domain name system
    - 13 primary server identities run by multiple organizations
    - Massively overprovisioned
    - Embedded into software - ensures a hierarchy for all end user interaction with service names
  - Multiple servers for each name on the DNS "tree"
  - Coordinated redundancy ensures end user can find resolve the name of the service they seek
- Many paths to your destination
  - The Internet is a network of networks, not a single thing
    - Networks peer with many others creating massive grid
    - If one path fails, another almost always available
  - Redundant and myriad connections ensure end users can find the services and resources they wish to connect with

# Internet and Users: Integrity

- Data integrity over the Internet
  - SSL, TLS, HTTPS - these secure protocols also help ensure the data transmitted is the same that was intended to be received by an end user
  - IPSec - suite of protocols and encryption that protect one or more data flows between IPSec peers
  - Technologies are ubiquitous in software used everywhere and allow for trustworthy Internet communications
  - End users are assured that data requested is accurate
- Integrity of communications signals
  - DNSSEC - cryptographic assurance that DNS query/responses include their published values
  - Ensures that ensuing communications are held between the end user and the intended resources
  - Protects end users from malicious redirection
  - Important to increase adoption for better user protection

# Internet and Users: Confidentiality

- Data encryption over the Internet
  - SSL, TLS, HTTPS - secure protocols that allow data to be transferred across the internet over encrypted connections
  - Supported by certificate technology that tie encryption to unique internet identifiers
  - Well-supported and standardized - allow software developers, website providers, and others to create easily used tools for end users to enjoy confidentiality on the Internet
- Encryption of communications signals
  - DoH/DoT - recent technologies that encrypt DNS queries themselves
  - Protects query data in-transit but not at DNS servers
  - Users may avoid surveillance and unwanted filtering
- ISPs and software vendors make decisions on which technologies to adopt for their end users

# Registration Data

- **Availability:** SSAD, RDAP
- **Integrity:** accuracy
- **Confidentiality**: Privacy and Proxy services

# Conceptual Framework For Stability

# Stability Conceptual Framework

- Are services delivered consistently and reliably?
  - **Consistent** - do you get the expected results from your interactions every time?
  - **Unique** - If you use a unique identifier to connect to something, is there just one proper result?
  - **Ubiquitous** - is the resource you are working with available everywhere or at least where it is supposed to be?
  - **Reliable** - can you access the data and services you need consistently over time?
  - **Responsive** - do you get the desired interaction accomplished in sufficient time?
- Decisions on Internet protocols, identifier policy, and provisioning of services are made to achieve these goals for the Internet's end users

# One World, One Internet

- Names and numbers on the Internet are uniquely assigned to ensure unambiguous and consistent results for finding data and services for end users
  - ICANN, ccTLDs and the domain name provisioning industry ensure the interoperation of all domain names
  - Root DNS servers provide a single, consistent foundation worldwide for the TLDs and individual names in the hierarchy
    - Alternative roots do exist for other protocols
    - DNS alternative roots have largely failed
  - RIRs distribute numbers to ISPs and edge networks
  - ISPs peer with each other to route traffic using a single set of addresses but multiple paths
  - ISP peering/routing decisions gear towards performance and availability for their end users
- Software is developed with libraries that utilize these principles
- End users can assume resources are unique without concern

# Provisioning - a key to the Internet's success

- End users expect the Internet to "just work" as long as they have a good connection
- Overprovisioning and redundancy allow for fast, reliable services available everywhere
- Massive peering and the underlying protocols ensure that data can find a path to get to its destination
  - The Internet was designed to always keep trying get data through, and ISPs route/peer with this in mind
  - ISPs usually make routing decisions for performance
- Content delivery networks (CDNs) move resources closer to users, distribute loads, and provide for unique content depending on user location
  - More recent development - uses routing tricks and co-location of equipment to move data closer to end users

# Call For Action

# Call For Action

- End users should insist on DNSSEC and DNSSEC enabled technologies.
  - signing your own domain
  - validate lookups
  - Express preferences for sites that are signed.

# Thank you

# Credits

- CIA Triad Diagram: https://www.ibm.com/blogs/cloud-computing/2018/01/16/drive-compliance-cloud/