DNS OARC

An information sharing and analysis
centre for the global DNS.
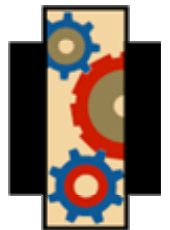
Background

- Information Sharing and Analysis Center

  – Concept originates with US homeland security efforts.

  – Allow industry participants to share potentially proprietary information during times of crisis.

  – ISACs in many different sectors

- *BUT*: ISAC not global enough, needed to expand the concept
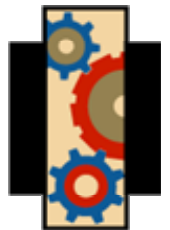
Key Functions

- Incident response
  - Shared, trusted platform for information exchange
- Operational characterization
  - Data collection infrastructure for consistency across time and multiple operators
- Testing
  - Interoperability of implementations
 - Debugging configuration and service options
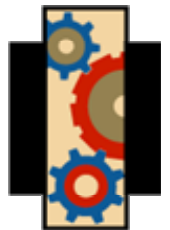
Key Functions (2)

- Analysis
  - Characterize normal functioning
  - Analyse attacks against DNS
  - Analyse backscatter to DNS from other attacks

- Outreach
  - Assist efforts to defend against attacks, malfunctions
 - Improved knowledge for operators everywhere
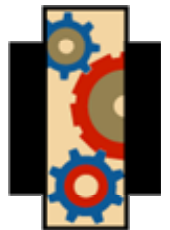
Information Exchange

- Vendors Need to Share Information

  – Information needed to solve problems during times of crisis may be proprietary.

  – Strong, binding membership agreement and trusted, secure information sharing platform insures proper coordination of efforts.

- Operators need to share experience too

- Complements CERTs, law enforcement
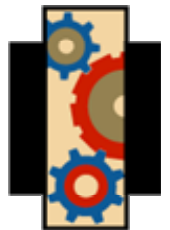
Secretariat for OARC

- OARC provided as public service by the Internet Systems Consortium

  – Not-for-profit corporation.

  – Long-term track record in public DNS operations insures credibility with participants.

- Other ISC public services:

  – BIND software

  – "F" root server.

  – OpenReg Software
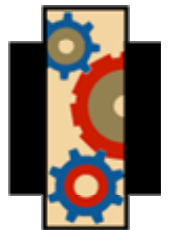
  – DNS Analysis and Measurement
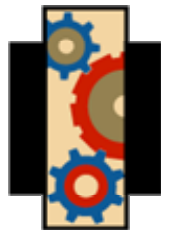
Analysis and Research

- ISC partnering with CAIDA for research and analysis.
- CAIDA well-known for ground-breaking analysis on the global DNS
  - Based at the University of California at San Diego
  - Funded by NSF, ARPA, vendors.
  - Strong credibility with ISPs, root operators, and others involved in operation of the global DNS.
  - Well-known for studies of performance, operation of root servers, DNS queries, measurement.
- ISC and CAIDA have jointly applied for NSF funding for a long-term research program.
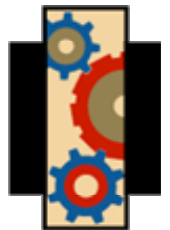
Membership

- Membership aimed at 4 classes of institutions:
  - Root and TLD operators.
  - Other large DNS operators (e.g., ecommerce providers).
  - Government institutions with responsibility for DNS operations (e.g., law enforcement).
  - Research and analysis institutions with a strong operational focus.

- Membership agreement
  - Fees based on number of Points of Contact assigned. $4,200/year for 3 POCs, $6,800 for 5 POCs.
  - Signed membership agreement required to insure confidentiality requirements are met.

Questions?