The Domain Name System Continuity of Operations

Apricot 2008

Taipei TAIWAN

28feb2008

Name Service Evolution

Bill Manning
"B" Operations
bmanning@ep.net

DNS Questions:1980-1989

- Does it work?
- Is it better than the alternatives?
- Who runs it?
- Who cares?
- Huge changes in software, capabilities, and underlying network technologies e.g. the Cambrian Era

DNS:1990-2000

- Defacto naming abstraction tool
- Rate of Innovative Change dropped
- Capacity augmentation was key
- User base changed

- Required changes required much more coordination and planning
- Planning for significant changes, some steps were taken

2001 -Stepping up to New Tasks

- Expanding system under given restraints.
- New DNS protocol requirements
  - IPv6
  - DNSSEC
- New operational challenges:
  - More servers – anycast!
  - Complexity of large installations.
  - Various types of attacks.

DNS Roots Today?

- Root Servers at 140+ sites
  - ... and counting
- Cryptographically signed data transfers
- Tight engineering cooperation
  - Regular meetings 3 times/year
  - Technical coordination
- Relationship with ICANN
  - Root Server System Advisory Committee
- Change control prevents rapid response

Attacks

- Yes, they do happen
- **THEY DON'T BREAK THE INTERNET!**
  - DNS is a **very, very** robust protocol!
  - Clients cache data, including lists of TLD servers
- Anycast gives decent protection
- Very close cooperation with software vendors, Internet service providers, law enforcement, and computer emergency response teams

- Successful Attacks can still be launched
  - **We lack a good "Continuity of Operations" Plan**

The Future?

- Still wider spread
  - Many corners of the world still under provisioned.
  - This is ongoing.
- IPv6
- DNSSEC
- Traffic analysis
  - Preventive measures

OR

Have the assumptions Changed?

- Mobility instead of Anchored
- Verifiable, Accurate data with Integrity
- Wisdom of a single namespace
- Implementation Choices reflect the 1980s design constraints
- Can new systems leverage off the existing system
- Do all addressable devices need a “name”

More thoughts for the future

- Synthetic devices may need names
- Other bindings may be useful, e.g. Name to Key or Key to Address
- Minimize Single points of failure
  - DDOS
  - Third Party Caches
  - Simple Delegation Hierarchy

Thank You