DNS Audits
Authoritative Checks

Bill Manning
bmanning@karoshi.com
What is it?

• its the public Internet
  – always on
  – always connected
• complimentary to other host counts
  – ISC/Network Wizards
  – RIPE
• periodic (quarterly/monthly) runs
• map the entire topology
Status

• IN-ADDR only - 1997-1999
• All delegations - 2000-present
• Only collecting data @ present
• working on reduction strategies
Core Engine

- Perl scripts - (what else :)
- built on DOC and prior audit efforts
- average run time 650+ hours
- May not be the best choice these days
- Augmentation
  - Server Fingerprinting
  - DNSSEC/NSEC walkers
Engine Tuning

• parallel execution reduces runtime to ~80 hours
• port to C/assembler (portibility?)
• limited by:
  – Query Time
  – Disk I/O
  – Bandwidth
History

• first audit done in 1993 - ONE shot
• asked NW to run the in-addr zone in 1996 - they refused
• testing in 2q1997
• first real run in 3q1997
• hammered by 8.1 acl deployment :)
• naive dependence on “version.bind” string :)
• a diverse group of funding agents :(
Data Considerations

• full zone transfers
  – Looking for NS records
  – too much data to keep, for some agents :(

• toss everything but soa & ns

• check each listed server for version
Next Steps

• Work on improving access to zone data
  – Use FTP for large zones
  – Contracts/NDAs for some zone data

• Educate admins for correct configuration

• What to do about private addresses in the DNS
  – RFC 1918
  – 6to4
  – Link-Local

• Getting more public analysis of this data
Why?

- Better linkage on delegation / announcement
  - In-Addr entries as sanity check on Whois & iRR data
- Provides a feedback loop to registries
- Track software diffusion rates
  - how quickly bad code is excised
  - how quickly new features are useful
- Track genetic diversity
  - Monocultures have interesting failure modes
  - Interoperability is hard to check
The datasets range:

- SOA/NS data only
- Server lists only
- Full zone copies

- Depends on who was funding when…:(

- Some common elements do exist though
  - tree structure
  - delegations in time
new things to do

• correlate delegations w/ announcements
• track use of BIND ACL use
• look for private address space “creep”
• track admin response time to CERT advisories
• anything else come to mind?
Issues

• DNS data is public!
  – Some zone admins think confidentiality is possible
• IPv6 reverse maps are going to be an issue
• The net is no longer “always on, always connected”
  – Split DNS
  – Multiple anchor points
Questions?