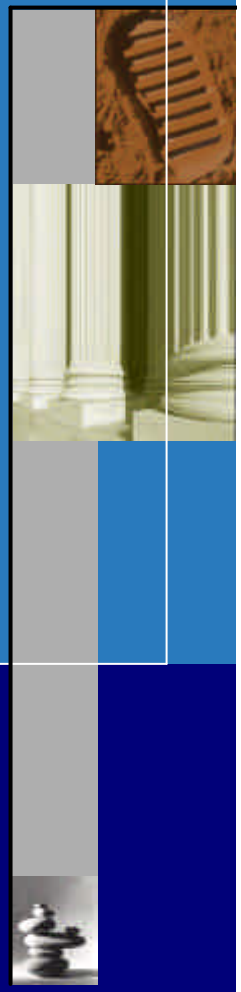
A Survey of ccTLD DNS Vulnerabilities

ITU ccTLD Workshop March 3, 2003
Jim.Reid@nominum.com



Nominum®

RATIONALE

- Health-check on DNS infrastructure
  - Now becoming a critical national resource
- Attacks on DNS servers becoming more common
  - October 2002 DDoS attack against the Internet root servers
- Objective is not to “name and shame”
  - Get a snapshot of where things stand today
  - Try to help fix the problems

Nominum.

THE GOLDEN RULE OF DNS

- NO SINGLE POINT OF FAILURE
  - Monocultures are **bad**…
- No one hardware and OS platform
- No one DNS implementation
- No single network
- No single ISP/carrier
- No one location or co-lo facility
- No single organisation
  - Avoid procedural and administrative failures

Nominum.

METHODOLOGY

- Used a Nominum system at LINX
  - Checked all ccTLDs
    - Delegation mistakes
    - Zone transfers
    - Recursive name servers
    - DNS software
    - Name server location
- Found 787 name servers for 243 ccTLDs

DELEGATION ERRORS

- Unresolvable names
  - 18 names (~2.5%) of ccTLD name servers could not be resolved!
  - ccTLDs are telling the world's name servers to look for servers that the ccTLD should know can't be found
  - Not critical but disconcerting
- Illegal Names
  - Using IP addresses instead of host names
    - One ccTLD does this for 3 out if its 4 name servers
  - 10 name servers listed as CNAMEs, not hostnames
    - Illegal according to the DNS protocol

MORE DELEGATION ERRORS

- Disagreement between parent and child
- The parent zone (i.e. the root) and the child zone (the ccTLD) should agree on the set of name servers for the delegation (TLD)
  - Not true for 155 ccTLDs: 65%
  - Mismatches are serious but not critical
    - There's always an overlap
    - ccTLD's name servers sometimes a superset of the root
  - Shouldn't happen for any important zone in the DNS

LAME DELEGATIONS

- Very serious problem
- Name server that should be authoritative isn't
  - In DNS jargon, such servers are lame
- Causes failed lookups
  - Lame server gets queried and can't answer
- Survey results startling:
  - 43 ccTLDs had at least one lame server
  - 2 had all their servers lame
  - Another 8 had half or more of their servers lame
- No excuses for this
  - Caused by administrator error, failure to use checking and reporting tools

Nominum.

RECURSIVE SERVERS

- Service queries from end clients and query other name servers
  - Can be made to query any name server for any name
  - Will believe what they are told, which may be lies
  - Will cache those answers and return them to clients
- An obvious evil for a ccTLD
  - Also has performance and resource penalties
  - No need **at all** for ccTLD servers to enable recursion
- 371 - 47% - of the ccTLD name servers have recursion enabled
  - They are vulnerable to cache poisoning attacks

ZONE TRANSFERS

- Tried to take a complete copy of the zone from each ccTLD name server
- Succeeded for 140 ccTLDs
  - Inconsistent policies
    - Some ccTLD name servers reject zone transfer requests but not all of them
- Why this is bad:
  - Resource drain (bandwidth & server)
  - Privacy/data protection concerns
  - Helps cybersquatters

FINGERPRINTING

- Identified the name server software in use
  BIND 8 364 Servers 47%
  BIND 9 268 Servers 34%
  BIND 4 42 Servers 5%
  UltraDNS 10 Servers 1.3%
- 144 using old versions of BIND8 - security concerns?
- BIND 4 is effectively dead
  - Some not even running latest (last?) version of BIND4
- BIND 8 is “in the departure lounge”
  - Not under active development

Nominum.

NAME SERVER CODE DIVERSITY

- Code diversity in ccTLDs could be better:
  1 DNS Implementation - 42 ccTLDs
  2 DNS Implementations - 97 ccTLDs
  3 DNS Implementations - 88 ccTLDs
  4 or more: 16 ccTLDs

LOCATION ANALYSIS

- Harder than first thought
  - Difficult to automate
  - No tools yet for linking AS numbers to IP netmasks
- Checked by hand for common address prefixes
  - => suggest single routing table entries
- 13 ccTLDs have all their name servers in one net
- 36 ccTLDs have at least 50% of their name servers in one net
- Loss of network route => no access to name servers => no access to ccTLD

FURTHER CONCERNS

- Agreements with slave server providers
  - SLAs, response times, monitoring, fault escalation
- Protection against DDoS attacks
  - Happens all the time to the root servers
  - Only a question of time for ccTLD infrastructure
- Improved monitoring of ccTLD servers
  - Already done for the root name servers

CONCLUSIONS

- High incidence of basic DNS administrative errors is surprising
  - Shouldn't happen for important zones like ccTLDs
  - Easy to prevent: tools & procedures
- Recursive servers for ccTLDs are **very** bad
  - Needless exposure to cache poisoning
- More work needed on
  - Monitoring
  - Service Level Agreements
  - Defence against Distributed Denial of Service Attacks