Network Path Problems in DNSSEC’s Deployment

Eric Osterweil
Dan Massey
Lixia Zhang
The Network Path and PMTU

• A network path is a sequence of links
  – Each link can only support packets of a certain size (MTU)
• The smallest MTU for a network path is its bottleneck (PMTU)
• Further limited by “middle boxes” (firewalls, NAT, etc.)
  – We overload the term PMTU to apply in these cases too
• Network paths that *do* support large packets may fail to deliver large DNS messages
It Matters Where You Look From

- NL NetLabs only has trouble with roughly 10 zones (graph on the left)
- At the same time, our SOHO router has PMTU problems with roughly 100 zones (on the right)
• We use a metric (defined in prior work) to quantify the “availability dispersion” of each zone
  – Captures how different each poller’s view of each zone is
• Using a weighted average over time, we see that most zones have suffered dispersion
"dnsfunnel"
Take a Look Yourself

dnsfunnel questsys.com.
The Nature of the Problem

• There is no silver bullet
  – This is an end-middle-end problem
• Network paths have limitations at various points
  – Not always just the sender or receiver side
  – If problem is at the sender/receiver, test and upgrade
• Resolvers specify buffer sizes that exceed PMTUs
  – EDNS0 buffer size ≠ PMTU size
  – More intelligent discovery and use of buffer size
• Name servers treat buffer sizes as path-capacity
  – How should they know better?
  – Where possible, reduce set sizes
What to do Tactically

• Download our toolkit that includes dnsfunnel: 
  
  http://vantage-points.org/

• Check your zones’ availability at: 
  
  http://secspider.cs.ucla.edu/
Thanks
Backup
As Seen From All of Our Pollers

- Green bars indicate the number of times a poller needed to do a PMTU walk
- Red bars indicate the percentage of times a PMTU was able to find a buffer size the allowed DNSKEYs to be received
“dnsfunnel”
Take a Look Yourself

- dnsfunnel questsys.com
- dnsfunnel ripe.net