NSEC3 Update

IETF 67, San Diego

David Blacka, VeriSign
What is going on?

- Workshop in Dulles, Virginia on September 18–20
- Draft is now at version -08
- Most open issues have been addressed
Dulles Workshop

• Purpose: Additional interoperability testing, testing attacks, discussion
• Tested NSEC3 signaling and traversing
• Tested transitions from NSEC->NSEC3
• Re-tested zone signing, loading, transfers
• Tested validation of “broken” packets
Dulles Workshop, cont.

• Tested:
  – 2 NSEC3-capable authoritative servers
  – 4 NSEC3 signers
  – 4 NSEC3 resolvers/validators

• No major surprises.

• Full report available at http://www.nsec3.org
Dulles Workshop, cont.

• Found one non-NSEC3 specific issue:
  – In NOERROR/NODATA proof validators must check that CNAME does not exist at QNAME, in addition to QTYPE (Issue 26)

• Workshop also generated:
  – Issue 24: Significance of algorithm numbers
  – Issue 25: NSEC3 and DNAME at zone apex.
  – Issue 27: Create flags octet
Changes from -06 to -08

• Added NSEC3PARAM RR (Issue 18)
• NSEC3 records cannot be queried for directly (Issue 11)
• Validators ignore NSEC3 RRs using unknown hash algorithms (Issue 23)
• Maximum iterations table based on verification speed instead of signing speed (Issue 9)
• Added NSEC->NSEC3 transition algorithm
Changes, cont.

- Update RFC 2672 to allow NSEC3 RR under apex DNAME (Issue 25)
- Check for CNAME in NODATA proof (Issue 26)
- Added flags octet, reduced iterations field to 2 octets (Issue 27)
Issues

• NSEC3 has an issue tracker
  – http://www.nsec3.org

• Almost all issues are closed.
  – This means that the draft editors think that the issue is addressed
  – Not that the issue cannot be discussed further
Open Issues

• Issue 24: Significance of Algorithm Numbers
  – Essentially, what does it mean when zone has both standard algorithm DNSKEY and NSEC3-aliased algorithm DNSKEY?
  – Proposed solution: Clarify section 2 “Backwards Compatibility”
Next Steps

• Anticipate one more draft version (-09)
  – Correct example zone
  – Edits for clarity
  – Address Issue 24

• Otherwise think we are done
The End

Questions/Comments?