DNSSEC
The Experience So Far

Chris Thompson
University of Cambridge
3 April 2012
A brief history of the DNS

✧ The DNS protocol developed 1983-1987
✧ RFCs 1033-5 remain the base documents
✧ Security was not a primary concern
✧ DNS use of UDP datagrams eases attacks
✧ Many attacks, many countermeasures
✧ Dan Kaminsky's attack method mid-2008
✧ Countermeasure was random source ports
A briefer one of DNSSEC

- IETF working groups started work c. 1994
- RFCs appeared c. 2000, but are obsolete
- Finalised in RFCs 4033-5, published 2005
- But there are later additions (e.g. NSEC3)
- DNSSEC is end-to-end, not server-server
- DNSSEC optional, zones signed/unsigned
- Validator classifies secure/insecure/bogus
DNS background at Cambridge

- Computing Service took cam.ac.uk in 1991
- Since 2001-2, most content from database
- Since 2005, most changes via DNS update
- Up-to-date BIND, compiled ourselves
- Few delegations at the DNS level
- Encourage stealth slaving within university
Implementing DNSSEC in 2009

- I have followed the DNSSEC saga for ...
- Post-Kaminsky, got permission to deploy
- Needed BIND 9.6 for re-signing, NSEC3
- Deployed DNSSEC validation June 2009
- Signed cam.ac.uk August 2009, more later
- Changed SOA serial number management
- Biggest problem: Windows stealth slaves
Advertising signed zones

✦ To validate keys, look at DS in parent zone
✦ And then up the tree, to a trust anchor
✦ But what if the parent is not (yet) signed?
✦ ISC invented DLV, and dlv.isc.org
✦ DLV zone acts “in loco parentis”
✦ Not everyone approves ...
✦ But in 2009, there was no alternative
Spread of DNSSEC since 2009

- The root zone was signed on 15 July 2010
- Some TLDs ready, e.g. Nominet for “uk”
- Verisign signed “edu”, “net”, “com”
- 91 out of 313 TLDs now signed (85 DS)
- JANET signed “ac.uk” in February 2011
- DS record for cam.ac.uk in April 2011
- RIPE, ARIN, APNIC signed reverse zones
- Our ERX reverse zones now avoid DLV
Network issues with DNSSEC

- DNSSEC relies on EDNS extensions
- UDP payloads are substantially larger
- This can lead to IP fragmentation
- Fallback to TCP will happen more often
- Defective firewalls often cannot cope
- Test using dns-oarc.net replysize service
- Unpatched qmail has problems
Can DNSSEC validation hurt?

- Improperly signed zones give SERVFAIL
- But if no-one validates, signing not tested!
- Advice to “gov” domain owners backfired
- There have been bugs in BIND's validation
- E.g. on signed to unsigned transitions
- And the “de” issue with DS/DLV conflicts
- BIND has no “negative trust anchors”
Key sizes, algorithms, and proving non-existence

- Using separate KSKs and ZSKs useful
- Officially only RSASHA1 mandatory
- But in practice so is RSASHA256, NSEC3
- BIND default 1024-bit ZSK, 2048-bit KSK
- We use 864-bit ZSK, 1280-bit KSK
- Use NSEC3 only if really necessary
Trust anchors and private zones

- Need trust anchors for root and dlv.isc.org
- RFC 5011 and BIND's managed-keys
- Signing disconnected zones (e.g. RFC1918)
- The “real” delegations (if any) matter
- RFC 6303 lists zones to be served locally
- We do not yet sign private.cam.ac.uk
- Or RFC 1918 reverse zones
Past and future developments

- We now use BIND 9.7+'s “auto-dnssec”
- BIND 9.9 (Mar 2012) has “inline signing”
- Support for DNSSEC from e.g. Infoblox
- End-to-end ought to mean stub resolvers
- DNSSEC helps ssh (SSHFP) mail (DKIM)
- But TLS certificates are the hot topic
- Chrome, and the DANE working group