

D N S S E C and D a t a P r i v a c y

D r W B l a c k

(with acknowledgements to Geoff Sisson)

c c T L D R e g i s t r y M a n a g e r s M e e t i n g

T u e s d a y , 2 0 th J u l y 2 0 0 4

Som e background . . .

- Ad hoc survey on CENTR GA mailing list in April
 - Question was: “How does the risk of zone file elaboration affect your registry’s attitude towards DNSSEC ?
 - Only four responses . . .
 - . . . even though multiple choice! :-)
 - So maybe no one cares?
 - Or maybe issue isn’t well understood?

D isclai m er

- N om inet is s ponsor of an Internet D raft (I-D) which proposes a *possible* rem edy
- . . . how ever this presentation is *intended* to inform rather than propagandise
- N ot m eant to generate F U D *!
- N ote to techies: som ewhat relaxed use of term inology follow s, e.g. “dom ain nam es” rather than “ow ner nam es” , R R sets, etc.

*“*Fear, Uncertainty and Doubt*”

(<http://en.wikipedia.org/wiki/Fud>)

What is DNSSEC ?

- Concise answer: an extension to the DNS protocol which uses cryptographic authentication to add security to the DNS.
 - Makes it effectively impossible to forge DNS replies
- 1. DNSSEC
 - RFCs 2535 – 2539, released in 1999
- 2. DNSSECbis
 - Current Internet Drafts:
 - draft-ietf-dnssec-intro-10.txt
 - draft-ietf-dnssec-protocol-06.txt
 - draft-ietf-dnssec-records-08.txt
 - Available at: <http://www.ietf.org/internet-drafts/>

W hat is D N S S E C (cont'd)

- D N S S E C
 - F ulfilled technical objectives but presented serious challenges to deployment
 - Specifically, key rollover was difficult
- D N S S E C bis
 - A dds “designated signer” (D S); perm its simultaneous use of two keys
 - Sim plifies key rollover.

NSEC Resource Records

- DNSSEC uses a type of DNS resource record (RR) called NSEC (“Next Section”)
 - Used to be called NXT
- From perspective of a “delegation-only” zone (typical of most TLDs), NSEC RRs serve as proof that no domain names exist between two alphabetically consecutive domain names
- Constitutes “authenticated denial of existence” of a domain name
- Analogy: like turning pockets inside-out to prove there’s nothing inside.

NSEC Resource Records (*cont'd*)

- Example: the DNS resource record:
nominet.co.uk. IN NSEC nominum.co.uk.
indicates that no domain name exists between
nominet.co.uk and nominum.co.uk
 - e.g. nominot.co.uk
- Nice, because minimises amount of work name servers
have to do
 - also means that private keys don't have to reside on name
servers, where they may be more vulnerable.
- Other ways to deny existence, but require more work by
name servers
 - makes hardware expensive
 - makes DDoS easier.

What's the problem ?

- NSSEC RRs can be used to “walk” the domain names in a zone file
 - provides a “compilation copy” of the domain names in a zone
 - similar to a zone transfer
 - can collect one name after another like a string of beads

A *(Fictional)* exam ple



bbc.co.uk

bt.co.uk

cat.co.uk

dog.co.uk

foo.co.uk

ggg.co.uk

xxx.co.uk

yyy.co.uk

zzz.co.uk

Example (cont'd)

- Demonstration Perl script available at:
 - <http://josefsson.org/walker/>

Why didn't we at Nominet "come out of the closet" on this issue earlier?

- Nominet's been aware of issue for years, but we were somewhat resigned to "feature"
- Believed that name server implementers would develop anti-abuse mechanisms, such as rate-limiting
- Perhaps overly-reliant on action by gTLDs
 - However, NSEC traversal does *not* appear to be perceived to be a major gTLD problem; ICANN requirements mean zone file data is already made available without significant barriers.

What changed?

- Intensity and creativity of abuse
 - More often seen with WHOIS, but NSEC RRs may change that
 - Use of unsecured proxies, sometimes chains of proxies
 - Probably many more unsecured resolvers than WHOIS/WWW proxies
 - Use of “bot-nets”
- Recent (and ongoing) litigation highlighted the the potential of problem .

What we did . . .

- Wrote Internet Draft which proposed one possible solution:
 - <http://www.links.org/dnssec/draft-laurie-dnsextnsec2-00.txt>
 - Obfuscated alternative NSEC RR so cannot be easily used to reconstruct contents of zone file
 - Intended as an alternative rather than a replacement
 - Appropriate only where privacy is a concern
 - In some places it would provide little additional privacy, e.g. e164.arpa (ENUM) and in-addr.arpa (reverse delegation) trees
- Substantially revised version of 2001 I-D by Simon Josefsson:
 - <http://www.watersprings.org/pub/id/draft-ietf-dnsextnot-existing-rr-00.txt>
- Working on patches for BIND and nsd
- Unsolved problems remain:
 - DNS wildcards may pose a problem
 - More work for name servers.

Consequences

- Timing was unfortunate – DNSSECbis drafts were in Working Group Last Call
- Prompted intense debate in IETF dnsect WG
- Ultimately recognition by WG that NSEC walking was a serious problem for some registries – especially in EU – which may prevent DNSSEC deployment
- Did not result in changes to the DNSSECbis drafts.

Consequences *(Cont'd)*

- Long-term solutions have been deferred until DNSSEC bis is out as RFCs.
 - Probably will involve a Type Code rollover (as DNSSEC bis did); is now popularly referred to as DNSSEC ter, after ID by Paul Vixie.

Next steps

- Watch these spaces:
 - Namedroppers (IETF dnsex WG) mailing list – archive available at:
<http://ops.ietf.org/lists/namedroppers/>
 - DNSSEC Mailing List – archive available at:
<http://www.cafax.se/dnssec/maillist>

Q U E S T I O N S ?

www.nominet.org.uk