DNSSEC and Data Privacy

Dr W Black
(with acknowledgements to Geoff Sisson)
ccTLD Registry Managers Meeting
Tuesday, 20th July 2004
Some 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?
**Disclaimer**

- Nominet is sponsor of an Internet Draft (I-D) which proposes a possible remedy.
- ... however this presentation is intended to inform rather than propagate.
- Not meant to generate FUD*!
- Note to techies: somewhat relaxed use of terminology follows, e.g. “domain names” rather than “owner names”, RR 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. DNSSEC bis
   - Current Internet Drafts:
     - draft-ietf-dnsext-dnssec-intro-10.txt
     - draft-ietf-dnssec-protocol-06.txt
     - draft-ietf-dnssec-records-08.txt
   - Available at: http://www.ietf.org/internet-drafts/
What is DNSSEC (cont'd)

- DNSSEC
  - Fulfilled technical objectives but presented serious challenges to deployment
    - Specifically, key rollover was difficult

- DNSSEC bis
  - Adds "designated signer" (DS); permits simultaneous use of two keys
    - Simplifies key rollover.
NSSEC Resource Records

- DNSSEC uses a type of DNS resource record (RR) called NSSEC ("Next Section")
  - Used to be called NXT

- From perspective of a "delegation-only" zone (typical of most TLDs), NSSEC RR s 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.
NS E C R e s o u r c e R e c o r d s  (cont’d)

• E x a m p l e: t h e D N S r e s o u r c e r e c o r d:
  nominet.co.uk. IN NSEC nominum.co.uk.
  i n d i c a t e s t h a t n o d o m a i n n a m e e x i s t s b e t w e e n
  nominet.co.uk and nominum.co.uk
  • e.g. nominot.co.uk

• N i c e, b e c a u s e m i n i m i s e s a m o u n t o f w o r k n a m e s e r v e r s
  h a v e t o d o
  • a l s o m e a n s t h a t p r i v a t e k e y s d o n ’ t h a v e t o r e s i d e o n n a m e
    s e r v e r s, w h e r e t h e y m a y b e m o r e v u l n e r a b l e.

• O t h e r w a y s t o d e n y e x i s t e n c e, b u t r e q u i r e m o r e w o r k b y
  n a m e s e r v e r s
  • m a k e s h a r d w a r e e x p e n s i v e
  • m a k e s D D o S e a s i e r.
What's the problem?

- NSEC 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) example

<table>
<thead>
<tr>
<th>Domain</th>
<th>Type</th>
<th>Name</th>
<th>Domain</th>
<th>Type</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>bbc.co.uk</td>
<td>IN</td>
<td>NSEC</td>
<td>bt.co.uk</td>
<td></td>
<td></td>
</tr>
<tr>
<td>bt.co.uk</td>
<td></td>
<td>IN</td>
<td>NSEC</td>
<td>cat.co.uk</td>
<td></td>
</tr>
<tr>
<td>cat.co.uk</td>
<td></td>
<td>IN</td>
<td>NSEC</td>
<td>dog.co.uk</td>
<td></td>
</tr>
<tr>
<td>dog.co.uk</td>
<td></td>
<td>IN</td>
<td>NSEC</td>
<td>foo.co.uk</td>
<td></td>
</tr>
<tr>
<td>foo.co.uk</td>
<td></td>
<td>IN</td>
<td>NSEC</td>
<td><a href="http://www.co.uk">www.co.uk</a></td>
<td></td>
</tr>
<tr>
<td><a href="http://www.co.uk">www.co.uk</a></td>
<td></td>
<td>IN</td>
<td>NSEC</td>
<td>xxx.co.uk</td>
<td></td>
</tr>
<tr>
<td>xxx.co.uk</td>
<td></td>
<td>IN</td>
<td>NSEC</td>
<td>yyy.co.uk</td>
<td></td>
</tr>
<tr>
<td>yyy.co.uk</td>
<td></td>
<td>IN</td>
<td>NSEC</td>
<td>zzz.co.uk</td>
<td></td>
</tr>
</tbody>
</table>

Nominet: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, NS ECC 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 NSSEC 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 potential of problem.
What we did ...

- Wrote Internet Draft which proposed one possible solution:
  - http://www.links.org/dnssec/draft-laurie-dnsext-nsec2-00.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 ID by Simon Josefsson:
  - http://www.watersprings.org/pub/id/draft-ietf-dnsext-not-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 — DNSSEC bis drafts were in Working Group Last Call
- Prompted intense debate in IETF dnsext WG
- Ultimately recognition by WG that NS SEC walking was a serious problem for some registries — especially in EU — which may prevent DNSSEC deployment
- Did not result in changes to the DNSSEC bis 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 I-D by Paul Vixie.
Next steps

- Watch these spaces:
  - Name droppers (IETF dnsext WG) mailing list – archive available at:  
    http://ops.ietf.org/lists/namedroppers/
  - DNSSEC Mailing List – archive available at:  
    http://www.cafax.se/dnssec/maillist
QUESTIONS?

www.nominet.org.uk