Security Considerations

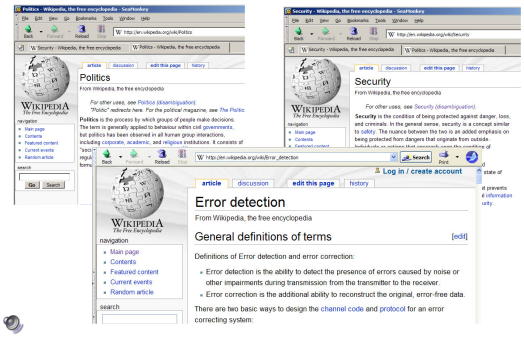
DNSSEC – Technical Workshop
European Commission, Brussels
5th February 2009.

Paul M Kane
Director,
www.CommunityDNS.eu

Background

- Paul Kane:
  - Working in the "Internet" industry since mid 1980's and with domain names registries since 1996.
  - On the Board of Directors of 7 software service delivery companies, one of which is a Back-end Registry provider to 14 ccTLDs – Group employs a total of 114 staff in UK, Japan and USA.
  - Am the General Manager of a few small ccTLD Registries.
- CommunityDNS – "Together, we can beat the bad-guys".
  - Anycast DNS is the technology, but protecting the Registry's data by effective monitoring, resolution and efficient software is the business.
  - Get as much authoritative DNS data as close to the user as possible.
  - 2008 – we beat all other Anycast service providers to win an EU Justice, Freedom and Security Project for the Prevention, Preparedness and Consequence Management of Terrorism and Other Security related Risks for the Period 2007-2013.
  - CommunityDNS has DNS servers in Austria, Belgium, Denmark, France, Hungary, Ireland, Luxembourg, Netherlands, Poland, UK and ..... – more countries welcome – just contact us.
  - If customers want we will support IPv4, IPv6 both with DNSSEC.

DNSSEC more Politics than Security?



DNSSEC – why and when?

- Cache poisoning:
  - Security Researcher *Dan Kaminsky's* approach to cache poisoning has been known about for many years.
  - In 1998 - CENTR recommend recursion be turned off – so TLD Registries authoritative Name Servers were never vulnerable to this attack;
  - Further down the DNS tree however, Kaminsky's approach of using the protocol against itself demonstrated it was possible to poison BIND, (the world's most popular "all-inclusive" name server platform) in under 10 minutes.
  - BIND's subsequent fix of UDP source port randomization patch was broken by a Russian security researcher, within 24 hours of its release, showed that it was possible to crack BIND's fix in under 10 hours using two laptops.
- Is DNSSEC ready to move from the semi-Research community to the real-world and what are the security benefits?

The theoretical benefits of DNSSEC

- Design team started work in November 1993 at the 28th IETF meeting in Houston;
  - Various refinements since then, how many more to come?
- End-to-end authentication of DNS data;
  - When it verifies authenticity "great", but what happens to the user's experience when authentication fails? Tools are currently under development to "inform" them why their Internet is not working!
- Relatively easy for TLD Registry to start serving DNSSEC signed records;
  - As a ccTLD registry operator we started a DNSSEC trial in 2004: many aspects to consider; Relationship Management: registry interface for key management, key revocation, name server management, BGP security monitoring, Registrar tools and training, ISP education and motivation, Customer education etc.

Operational considerations of DNSSEC

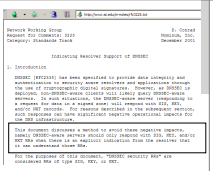
- Users Expectations;
  - They want their "Internet" to work – DNSSEC verification failure impedes the user "always-on" experience.
  - Users almost accept a trade-off between certain Security compromises in favour of ease of use and resilient functionality.
- Registry considerations;
  - Today registry has relationship with Registrant via Registrar: Domain holder, Admin Contact, Technical Contact, Billing (Registrar) Contact and with DNSSEC a new contact – Key Management Contact/Role;
  - Key Management, including Roll-over empowers the highly technical Key Management contact to effectively control the accessibility of the domain and by-pass the "authority" of the other contacts;
  - Registrars want to profit from (easy) domain registration and prefer someone else to take liability for name's DNSSEC operation.
  - ISP's seem slow to adopt DNSSEC as it brings responsibility and duty of care with little financial benefit.

Known vulnerabilities of DNSSEC

- RFC 3833, Section 3 (2004):
  - trivial zone configuration errors or expired keys can cause serious problems;
  - DNSSEC significantly increases the size of DNS response packets; among other issues, this makes DNSSEC-aware DNS servers even more effective as denial of service amplifiers;
  - DNSSEC answer validation process increases the resolver's work load and in some cases will also need to issue further queries, magnifying load with query re-tries.
  - DNSSEC's trust model is almost totally hierarchical [so to ensure resilience the Root servers need operational independence].
  - DNSSEC Key rollover [without service disruption] is really hard. Running old and new keys in parallel for a period of time aids transition, but where key revocation takes place because of Key compromise, disruption to a signed zone is hard to avoid.

Follow the Standards to avoid disruption

- RFC 3225 (2001)
  - clearly specifies a method to avoid negative (bandwidth) impacts of DNSSEC deployment;
  - Respected until 2008, then ignored in BIND 9.6 as the "DO" (DNSEC aware) flag now turned ON by default even though the verification path is fragmented.



  - Nothing is broken - however the effect is magnitudes more data ("noise") in the DNS response which is simply discarded by Client as verification does not occur.
  - A "noise" fix is soon to be announced by BIND in their next Name Server version which proposes to use an existing second flag saying "I am DNSSEC aware and I can verify, please send me the whole data-set".

Broadband Routers and Firewalls

- Hardware issues - 24 (home) DSL Routers examined by CORE competence and Nominet:
  - Report indicating that 6 units (25%) operate with full DNSSEC compatibility "out of the box."
  - 9 units (37%) can be reconfigured by the technically aware to bypass DNS proxy incompatibilities.
  - Unfortunately, the rest (38%) lack reconfigurable DHCP DNS parameters, making it harder for LAN clients to bypass their interference with DNSSEC use.

- Useful Report but only a transitory problem
  - In time hardware vendors will fix packet fragmentation.

Commitment to "absolute" Time

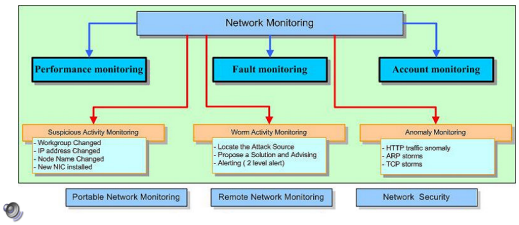
- NTP is a protocol designed to synchronize the clocks of computers over a network
  - Standard DNS only knows about "elapsed" or "relative" time.
  - DNSSEC relies heavily on absolute synchronisation at both ends - validating resolver and the entity creating the DNSSEC signatures;
  - Internet based NTP uses UDP packets which has no security and is relatively easily hacked remotely. (latest bug found 8/Jan/09)
  - Bad time syncronisation (outside of limits) will cause DNSSEC verification to fail.
- External Time source like GPS Receiver Clocks

To avoid vulnerable NTP servers DNSSEC operators use external GPS antennas to syncronise time. (Financial investment - pulses accurate to +/-1microsecond of UTC)

To reduce disruption a GPS Receiver should be externally mounted at each Client/Server Data Centres

Secure DNS is about network monitoring

- Anycast service delivery
  - Managing Anycast cloud represents approximately 30% of the job and is technically relatively easy.
  - 70% is network monitoring, looking for "bad" guys who seek to change DNS data for personal gain.



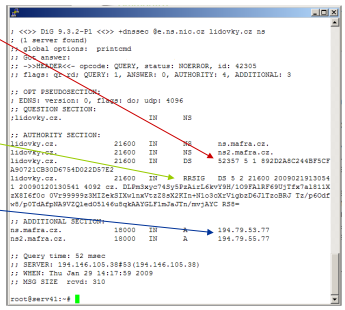
Real world DNSSEC Architecture weakness

- Tricks the "bad-guys" use - Glue Records:
  - In DNSSEC Glue records are unsigned - so using standard cache poisoning techniques they can manipulate a record to inject false IP address data to force the DNSSEC verification fails – User has no service ie DoS;

  Another approach used to "confuse" DNSSEC:
  - Bad guys use BGP poisoning to grab traffic and present themselves as authoritative for an IP address within the user's vicinity;
  - They create a DNS Proxy server to grab a signed DNSSEC record from "real" authoritative DNS server and present it themselves to the user;
  - If the sub zone is not signed they can change the A or MX records to point to a fake site/server
  - If End-to-End is signed they change glue records to point to a fake name server and inject false data to trigger verification failure.
- Possible perpetual Denial of Service:
  - DNS server will cache "failed" DNSSEC verifications resulting in the domain being deactivated until TTL expires – thereby widening the range of DoS attacks.

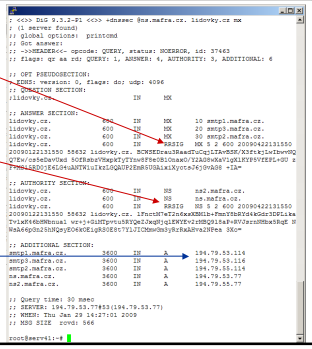
Brief review of DNSSEC a records…..

- The Public Key of the LIDOVKY.CZ domain is signed by nic.CZ
- Glue records are unsigned and can be corrupted



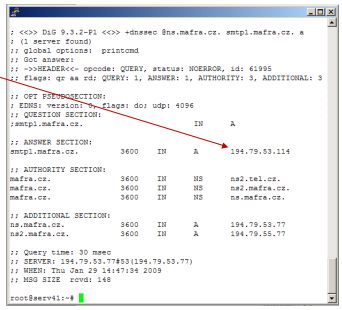
Drilling down for mail …….. signed

- LIDOVKY.cz MX record is signed
- LIDOVKY.cz Name Servers records are signed
- Glue Records are NOT signed – so could be subject to poisoning



Mail records…….. unsigned

- LIDOVKY.cz uses: smtp1.mafra.cz
- NONE of the records are signed
- Even if they were the IP addresses could be manipulated to trigger a DoS attack



ENISA Workshop Summary - 12/13 Nov 2008

- Academically DNSSEC is interesting and requires:
  - Exacting Technical standards be followed;
  - End-to-end validation tree – partial signing is insecure and can be manipulated;
  - A willingness of customers to deploy and pay for additional technical service cost – market seems reluctant;
  - Where DNSSEC verification fails – leaving the user with a blank screen is not an option at political level – tools are currently being built.
- DNSSEC version of today is considered work in progress:
  - The learning curve is valuable but current version is probably too brittle and many things can go wrong;
  - Need for end-to-end Testbed in a managed trial;
  - Signing the Root may have benefits but Network Resilience requires that there is no single point of control/capture so there is a requirement for multiple methods of verification.

Suggested Next Steps

- Testbed for definite period:
  - Things **WILL** go wrong – identify what they are in an official testbed;
  - My concern is DNSSEC **WILL** break users normal Internet "always-on" experience - their Internet **WILL** turn off when DNSSEC verification fails:
    - Unacceptable politically (both International and Nationally)
    - Unacceptable ISP service (so users need tools to choose)
    - Users are lead by "geeks" up the "creek" and dumped with "broken" Internet and a blank screen – "geeks" credibility destroyed, no second chance.
  - Good Management – "don't put all eggs in same basked" – have a second way to use the Internet – "with" or "without" error detection.
  - Application developers need to access BOTH systems – use two trusted locations to ROOT zone data (yep - two sets of name servers) – example:
    http://www.internic.net/zones/named.root (current and no error detection) and http://www.internic.net/zones/DNSSEC-named.root (with error detection).
- DNSSEC **will be** re-engineered, let us all make it work **better!**

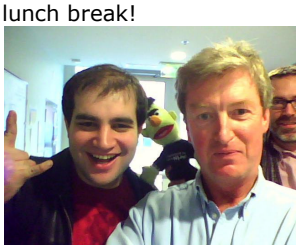
References

- RFC's:
  - Known issues with DNSSEC - http://www.ietf.org/rfc/rfc3833.txt
  - Indicating DNSSEC aware http://www.ietf.org/rfc/rfc3225.txt
- Nominet's DSL Router report:
  - http://download.nominet.org.uk/dnssec-cpe/DNSSEC-CPE-Report.pdf
- CommunityDNS' customer Monitoring suite:
  - http://www.communitydns.eu/partner_tools.html
- nic.SE DNSSEC Training day – 19th Feb, Stockholm:
  - http://ws.edu.isoc.org/helpfiles/workshop_info_main.php?id=459

Paul.Kane AT CommunityDNS.eu

Thank-you for your attention!

Enjoy the lunch break!



Dan Kaminsky, "Bert" and I join you from the two-day Global DNS Security, Stability and Resilience Symposium, Atlanta, USA

Paul.Kane AT CommunityDNS.eu