Some DNSSEC thoughts

DNSOPS.JP BOF
Interop Japan 2007

Geoff Huston
Chief Scientist, APNIC

June 2007

The DNS is a miracle!

You send out a question into the net ...

And an answer comes back!

Somehow

- But ...
  - WHO provided the answer?
  - Is it a REAL answer?
  - Can I TRUST the answer?

DNSSEC – The Motivation

- How can a DNS resolver tell if a DNS response can be trusted as **authentic**?
- Is this the **correct** DNS response?
  - Has it been altered?
  - Has it been truncated?
  - Is it hopelessly out of date?

DNSSEC – The Theory

Sign and publish ***everything***!

- Every DNS zone has associated key pairs
- Each zone publishes:
  - The public key (DNSKEY RR)
  - Private-key signatures of all RR Sets (RRSIG RR)
  - Private-key signed “gaps” in the zone file (NSEC RR)
  - Hashes of the public key of child zones (DS RR)

So you take a small zone….

```
TTL 86400
$ORIGIN        dnssec.potaroo.net.
@              IN     SOA    dns0.potaroo.net. gih.potaroo.net. (2006090803 3h  15   1w   3h )

; name servers
             IN     NS     dns0.potaroo.net.
             IN     NS     dns1.potaroo.net.
;
; subdomains
;
sub            IN     NS     dns0.dnssec.potaroo.net.
             IN     NS     dns1.dnssec.potaroo.net.
;
www             IN     A      203.50.0.6
bgp            IN     A      203.50.0.159
bgp2            IN     A      203.50.0.33
dns0           IN     A      203.50.0.18
dns1           IN     A      203.50.0.6
;
; wildcard
;
*             IN     A      203.50.0.18
```

And turn it into a big zone...

```
dnssec.potaroo.net.     86400   IN SOA  dns0.potaroo.net. gih.potaroo.net. (
                                        2006090803 ; serial
                                        10800      ; refresh (3 hours)
                                        15         ; retry (15 seconds)
                                        604800     ; expire (1 week)
                                        10800      ; minimum (3 hours)
                                        )
                        86400   RRSIG   SOA 5 3 86400 20061008080832 (
                                        20060908080832 3755 dnssec.potaroo.net.
                                        syLogFkxP1KlEkYp4Pic6qgW1Nr16powlzx+
                                        VbpdA/erzxRdARd1l77F56N7TB+v3aS82aLh
                                        BLIN+f0MzHEo/JNWVl0xjn95pRDd3gyZSoE+
                                        aWG21MokMbTBxF2pYmFA1ENNKKK+pSXuXvsS
                                        dAP+kcVqT6PfO67+m2chsqbh+uA= )
                        86400   NS      dns0.potaroo.net.
                        86400   NS      dns1.potaroo.net.
                        86400   RRSIG   NS 5 3 86400 20061008080832 (
                                        20060908080832 3755 dnssec.potaroo.net.
                                        p2kKLK4gzlm8nkr4lpXyz4FirWWXtiyXc5X/
                                        Ns2NYC3CNYDNIRFHzEI14RZO08R9z4aoQlfO
                                        jXidiJZ2BgxzmykVJUaA7AwGirVtr+6wDJrd
                                        if9tm7UdYN2powrP9o2lq0DKhwYk8i4Dyjdd
                                        9kwt7/x44ZECzEj7w30GfW4uvy8= )
                        10800   NSEC    *.dnssec.potaroo.net. NS SOA RRSIG NSEC DNSKEY
                        10800   RRSIG   NSEC 5 3 10800 20061008080832 (
                                        20060908080832 3755 dnssec.potaroo.net.
                                        h75DS6C1lGLPRbqtz9+KV4oSuidA+Bdt6geq
                                        q6NRrneNGA6Rr00FK4Td9AQS1+JpM3KriDl5
                                        LKqQM7yMarC7aE3v/23iW9YqFv3Z6PpjW7Ze
                                        oEhaLNCV3kG4tVmILsoGEp/EWtgNTnXkJdkD
                                        hW+o91s7XVnGmO7m9JkUOu8sS2E= )
                        86400   DNSKEY  256 3 5 (
                                        AQO8xvbN4hZ8bn926wpM8c9Uqqhqcf45v73k
                                        4J/YSu+6o/QsPCKwJoDYxMH3s5Z0NJlgLUQs
                                        cIZZKDYVHPW3Txt59bHrn739osnQ80RbOGVT
                                        H/Vi//L3BGjZrZr+PWtH2Vb3wIhrujMej2m4
                                        E2Mth/XjSDAhYZVWCNhJG0nPH6G6Ww==
                                        ) ; key id = 3755
```

Wait - there’s more ...!

```
 86400   DNSKEY  257 3 5 (
                    AQPSOR9BUnuQQ8ien6WibaSsKddzZstW4TEu
                    JrSzezQL79DFqHeOvVuhJr+9JMQmJuQGUjVc
                    XDG1gBRQboiFJ6e+G6sibIKlkzXCLSX7O9Yq
                    Ytyv1AMyEbYWLTwRvKojZSZr2LyKqeKGFqWd
                    oA8a1M6XRuChBlwxMwo5I5fsedIyYw==
                    ) ; key id = 29022
            86400   RRSIG   DNSKEY 5 3 86400 20061008080832 (
                    20060908080832 3755 dnssec.potaroo.net.
                    EMXe20wX8CNOeAg1iexEMSlGUuApeIB/zW1z
                    pHhZ+I/9YFE2bmmWaj6+jtfMMW8tvjlqdEFH
                    8TOihsMaPhu0nMQnqTrKTNS4Y4DkHqt05N6a
                    3yS1h/ufRfBDn2rA5EquVNGZM6TRI0iweDSn
                    1HsWy5+FiQcCFubsVJjCyqG/RXo= )
            86400   RRSIG   DNSKEY 5 3 86400 20061008080832 (
                    20060908080832 29022 dnssec.potaroo.net.
                    plmpAtyiQINPi0RcibIcry9eofJhvm6mkxZS
                    nL5Qb4x/g+DC02kXMhFCsVvNSU9ATAwRIOhY
                    PG85LaC7FdfWdOud5I+AVvVPRB+8aX1scS/8
                    /kQ5AbJuxT3b6ezCEhu2FSuRKN3uskV5Af4N
                    1nBBVmFWd7vXR53Q6KCucWjBvmg= )
*.dnssec.potaroo.net.   86400   IN A    203.50.0.18
            86400   RRSIG   A 5 3 86400 20061008080832 (
                    20060908080832 3755 dnssec.potaroo.net.
                    UTLlJPY60iaVo8skJKbljkF+Dz0ZFJiPGSLM
                    EmmzHVlYNeIjpQNK/o5jcIdDv7S4MZ+MJg31
                    MLPXuStBWe8ElfwU4w+eQX38dXP1fPs2Mjz2
                    RyG/dw2krgvVRfQDa27UJVurxDxoQTykEwW7
                    yYzAdA6oVflEkjyTF8O/CxrGVy0= )
            10800   NSEC    bgp.dnssec.potaroo.net. A RRSIG NSEC
            10800   RRSIG   NSEC 5 3 10800 20061008080832 (
                    20060908080832 3755 dnssec.potaroo.net.
                    ThBINgb7kHEq5t+wunmN/uTxlE5Z3nxI29e9
                    eFFidmBmMo459/oXeuc8w8kh9U0X2TQ1og8L
                    3GQwLNO75JrbsgMOSGzhNVD5b7Yj7PZNPWa7
                    M4O8z7ok3Dru5XOYf4NV5fORUsvHhBnOBr+/
                    6wTSdnpI/mQvGk5EmCKPwkvhzqE= )
bgp.dnssec.potaroo.net. 86400   IN A    203.50.0.159
            86400   RRSIG   A 5 4 86400 20061008080832 (
                    20060908080832 3755 dnssec.potaroo.net.
                    BjQFfiLaiOxP4rKIzT9OvteuVR3kR2NBYZgM
                    WMQxbSK6X4b84hE6HTRparY71bXXBvcKXIt7
                    MpWX97m1A9KScR7b37h084ZE1I6b86eaN3f9
                    Ad+9X1NXPw/RdrQZXby5xkyNSB0oIpM8R0Jz
                    kKGGi+OO5tn7O3TyBWMrlCznlaA= )
            10800   NSEC    bgp2.dnssec.potaroo.net. A RRSIG NSEC
            10800   RRSIG   NSEC 5 4 10800 20061008080832 (
                    20060908080832 3755 dnssec.potaroo.net.
                    SjjK2OpKnv514pUd0cfTMkgpqggljvcf+1NP
                    fizuFXMjOewJbdskKxE9FaRHwrDNvQpnwdyy
                    adgv+TBRLZhtHr1pO7aFfPyXCnsABffnPhWc
                    0s/xb1mAhAmPtf3f7Ri/CxrF5HFQF/lHHbHW
                    UUHzU2dkM8wOHzkGP/OPv5oNDOo= )
bgp2.dnssec.potaroo.net. 86400  IN A    203.50.0.33
            86400   RRSIG   A 5 4 86400 20061008080832 (
                    20060908080832 3755 dnssec.potaroo.net.
                    fuYkcujF/miEDcfSEPPAC/5wvYg6MmEqmlsg
                    xFTwDykT0otCSdsy5R/20meDtWbYWqwI1Wb5
                    7zTuBmSJprklTieq69j8Ptr4y3JGEsNeGA14
                    1fDMpqdT29kgvWJHKiZyEJ7Hj2zV9WuOrpu6
                    6hzW7pKz/xm9+Xv2ssx+u5nfrXU= )
            10800   NSEC    dns0.dnssec.potaroo.net. A RRSIG NSEC
            10800   RRSIG   NSEC 5 4 10800 20061008080832 (
                    20060908080832 3755 dnssec.potaroo.net.
                    S+X4oHey+hizmSF8d73877qYGK782uJzLgOA
                    dHnOD9RC0SolSriKfSD+l/q+47ckBhsaMx5B
                    9jMTRwor1fKZH8XKKyiNsuQjJqHi84sh2ZeK
                    fGmGPEZpDZR+Pk2biQSRpJo9tH29B0fsSE/O
                    fGDjImgkRhujnMlA/7RA1OilPF0= )
```

```
dns0.dnssec.potaroo.net. 86400  IN A    203.50.0.18
            86400   RRSIG   A 5 4 86400 20061008080832 (
                    20060908080832 3755 dnssec.potaroo.net.
                    LpbfDJtud6wqXVLnurpxkCuYtiFakQ0HFkIF
                    qJfs/R9xGwNizeS4f2+dR/rGnwxTDw522qdT
                    JFIBXbBR9RG9pSEqOCk/ivNSF8dPc7URbI4e
                    E0RWkgf9fE87x6cd2CHEaOrcgHDXbCZX594R
                    oWeutR9WohUPovs0aT1fOt2C9Gs= )
            10800   NSEC    dns1.dnssec.potaroo.net. A RRSIG NSEC
            10800   RRSIG   NSEC 5 4 10800 20061008080832 (
                    20060908080832 3755 dnssec.potaroo.net.
                    fGmGPEZpDZR+Pk2biQSRpJo9tH29B0fsSE/O
                    fGDjImgkRhujnMlA/7RA1OilPF0= )
dns0.dnssec.potaroo.net. 86400  IN A    203.50.0.18
            86400   RRSIG   A 5 4 86400 20061008080832 (
                    20060908080832 3755 dnssec.potaroo.net.
                    LpbfDJtud6wqXVLnurpxkCuYtiFakQ0HFkIF
                    qJfs/R9xGwNizeS4f2+dR/rGnwxTDw522qdT
                    JFIBXbBR9RG9pSEqOCk/ivNSF8dPc7URbI4e
                    E0RWkgf9fE87x6cd2CHEaOrcgHDXbCZX594R
                    oWeutR9WohUPovs0aT1fOt2C9Gs= )
            10800   NSEC    dns1.dnssec.potaroo.net. A RRSIG NSEC
            10800   RRSIG   NSEC 5 4 10800 20061008080832 (
                    20060908080832 3755 dnssec.potaroo.net.
                    fxw5MRcKkjR6bcRBaD4u/28sOLKZbVVTjYas
                    1dBcYyx0aW3lIUpvyIsjERU+oEG+g2DUQui+
                    2LA6PVntaCbKWfezwGkBtZBGKbwUcfNCdEa7
                    dNKQv3Aki5qGw1EAlkbahKt1FGbQLwO/WI4g
                    JFmOpYfcmaLtZdhgyWX60KBGIoY= )
dns1.dnssec.potaroo.net. 86400  IN A    203.50.0.6
            86400   RRSIG   A 5 4 86400 20061008080832 (
                    20060908080832 3755 dnssec.potaroo.net.
                    C1NTVm64mJDTDpM+aX07OLWhi92G9l5hkiW5
                    QbBmmITLq1x7QhMpasSPh41PRpa+teyeByFl
                    /46QGRpVb8IP4KmpbURd1YkPwAJbBBwb2Q+s
                    dXA6vfz3R/GSa62vSb2aCPfpvAAPkE3Hs66m
                    DF3DwVONpGuSgAWpn3A3H+1KbQs= )
            10800   NSEC    sub.dnssec.potaroo.net. A RRSIG NSEC
            10800   RRSIG   NSEC 5 4 10800 20061008080832 (
                    20060908080832 3755 dnssec.potaroo.net.
                    RfjymANoHG3TQ909fU/lenv3GsIZtEqR6fs7
                    fa/KJ4o4/OZU7+/VGz3CgUwBOLeMBab9f+Yr
                    KuFi83KvAt/W4E0nGxeDwgtnkTzUQJpkv7lA
                    AStqMIrqsZc8FyGJuZPJgU8Fzvn7+Ju7qsPU
                    Ntwi658ZRKoUl/K7uok6O7HmGSE= )
sub.dnssec.potaroo.net. 86400   IN NS   dns0.dnssec.potaroo.net.
            86400   IN NS   dns1.dnssec.potaroo.net.
            10800   NSEC    www.dnssec.potaroo.net. NS RRSIG NSEC
            10800   RRSIG   NSEC 5 4 10800 20061008080832 (
                    20060908080832 3755 dnssec.potaroo.net.
                    XNgHeGnZnmdg8AwHcnsvW6DzZEtnB0n5HVpk
                    1m2/oFoVgFr7MBuJT1t0beN8p/2zMuLF3Wad
                    HLmwLX0GqYBE/f+6afIA33aWTrLkuB11cmUj
                    iEk/4xMKAUgRAN04V6jOvVDnyESXY6g6afd3
                    J9yhhNvDukG3/8Iq1bUyVlRSKz8= )
www.dnssec.potaroo.net. 86400   IN A    203.50.0.6
            86400   RRSIG   A 5 4 86400 20061008080832 (
                    20060908080832 3755 dnssec.potaroo.net.
                    gWXzDRdiVRWxMCseWPQ2oi0QIHQxMZHT+Qj+
                    nk+tJMW3gvEVH+iP6uLGkwewywey8Ek1bLMe
                    Uwqlh6z8B35pBBn0hljwO3xO0Ly3ELHvtHUB
                    Q/2/bDbFaFDaXNA5IQn8I4RGLuaExDKq0dIF
                    tL/hq9y4rNHg7WTcNw9Q3pRfNUA= )
            10800   NSEC    dnssec.potaroo.net. A RRSIG NSEC
            10800   RRSIG   NSEC 5 4 10800 20061008080832 (
                    20060908080832 3755 dnssec.potaroo.net.
                    LRLFqls+FF2DqvuPOrnloRe6OclswCG/RL38
                    X1NLOshkpYjK4GcCsgsoyYCxH2vvmt2va+OU
                    RqVgL06brBizmmG7raS4kK9yd0bP+91CikWF
                    HuN8GOLjZ0Sel8CtyOeahtjy7cdqVovPkcje
                    P1yjDR8cI58wVsdvSCWlaoeCx9k= )
```

DNSSEC – Signing a Zone

- Generate a keypair
- Generate a Key-Signing keypair
- Load the keys into the zone
- Use a zone signing utility to sign **every** RR in the zone, and to sign **every** name gap in the zone
- Update the parent zone with the child’s public key hash
- Publish the zone with a DNSSEC-aware name server

DNSSEC – DNS Response

- The *Additional Information* section in a DNSSEC response contains:
  - a **DNSKEY RR**, and
  - an **RRSIG RR** for a data response, or
  - an **NSEC(3) RR** response for a “no such data” response

DNSSEC – Response Validation

- Validation of a DNS response:
  - Did the matching private key sign the RRSIG RR?
  - Does the hash match the RR data?
  - Does the public key validate?
    - Does the parent have a DS RR?
    - Has the Parent signed the matching RRSIG RR?
    - Does the parent’s key validate?

    - Loop until you get to a recognised “trust anchor”

This interlocking of parent signing over child is a critical aspect of the robustness of DNSSEC. It’s also DNSSEC’s major weakness in today’s partial DNSSEC deployment world

Some initial questions:

- How do you know if this is current data, or a replay of older stale data that was signed with the current key?
- How do you know that a zone is DNSSEC signed?

  (As distinct from man-in–the-middle attack that is stripping out DNSSEC information from DNS responses)
- How do you roll keys over?
- How do you revoke keys?
- What’s NSEC3?
- What’s a “trust anchor”?

“Trust” is a very tricky thing

- In the ideal world ALL the DNS would be DNSSEC signed
  - As long as you have the current root DNSSEC public key as your trust anchor then every DNS response can be validated by simply walking backwards up the name hierarchy to the root

- But this is really not the case:
  - Only a few zones are signed
  - And you don’t know which ones!
  - So which trust keys do you load and from whom?
  - And when should you update these keys?
  - Right now DNSSEC is pretty much unuseable as a generally useful tool

Status of DNSSEC

- The DNSSEC spec is over 10 years old
- Interest in deployment of DNSSEC has been very limited
- The trust model makes use of DNSSEC to validate responses in a partial deployment world very frustrating
- So few clients use DNSSEC to validate DNS responses
- So few zone publishers see any benefit in signing their zone
- And nothing happens…….

- Will DNSSEC ever get deployed across a meaningful and generally useful proportion of the DNS world?

One Opinion

DNSSEC Positives

- DNSSEC makes the DNS harder to attack
- Trust injection into the DNS can be leveraged for more than just trusting DNS responses
  - Use the DNS to pass other keys, SSL certs, other data objects, all secured by DNSSEC
- DNSSEC can avoid the overheads of yet more special-purpose PKIs

The DNS is a critical point of vulnerability in the network’s overall model of integrity of operation -- DNSSEC can really help here

DNSSEC Negatives

- DNS Zones get VERY LARGE
  - x 10 in size
- DNS responses can get VERY LARGE
  - amplification attacks become more effective
- DNSSEC Zone management is complicated
- NSEC implicitly exposes the zone contents
- NSEC3 is extremely obscure and challenging to verify
- Who can use the signed answer, and how?
- Today’s partial deployment trust model is useless

DNSSEC represents a significant investment on the part of the server with unclear benefits for a potential client

My Opinion

- The DNS would be really very useful and far more straightforward to use for validation if everyone deployed DNSSEC

- The DNS would be far more cumbersome, far more complex to manage, and far more error-prone to operate, if everyone deployed DNSSEC

- And for as long as only some of us deploy DNSSEC its not of much value at the moment!

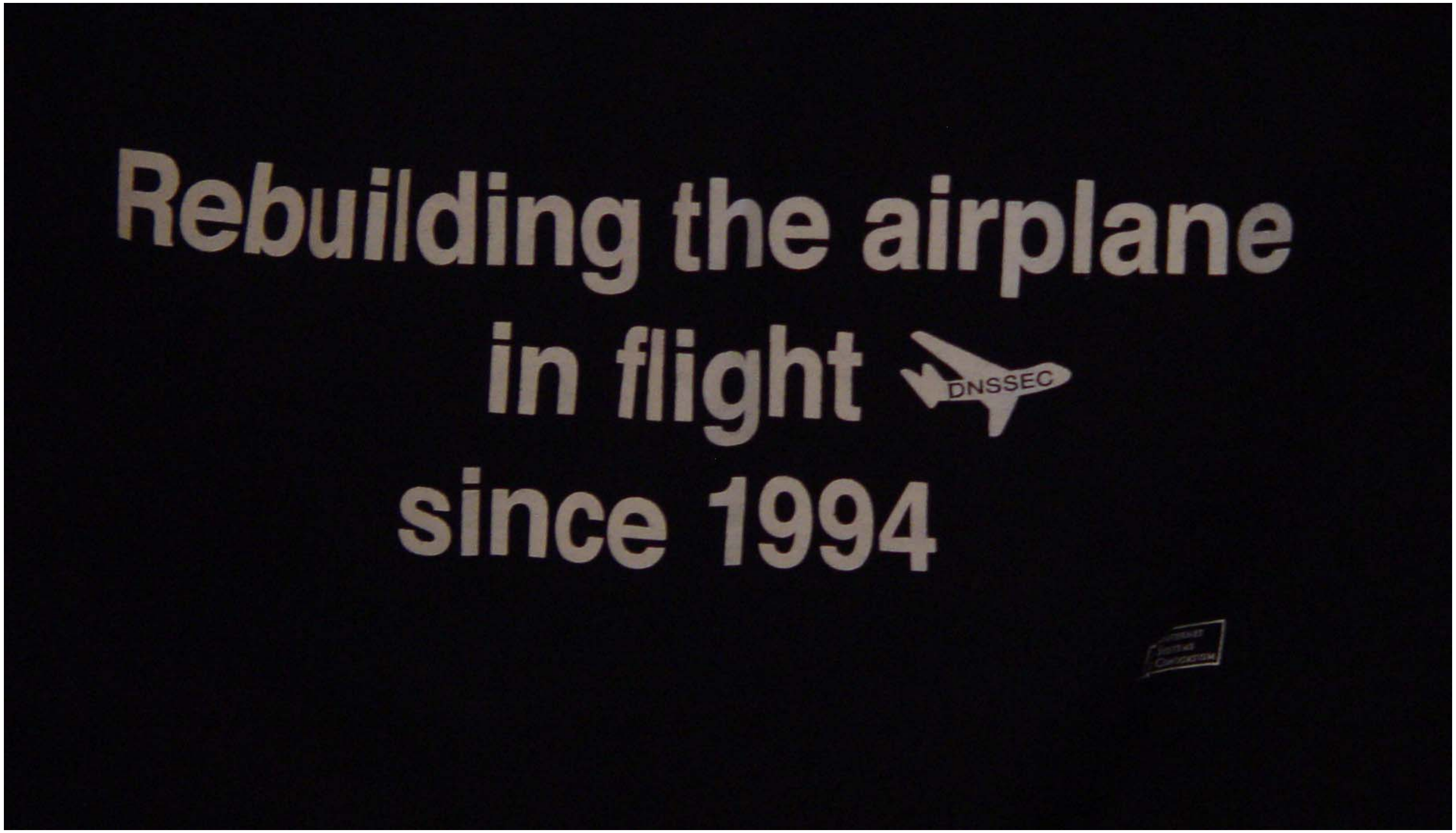
Next Steps for DNSSEC?

- Complete, top down, all zones, DNSSEC deployment looks like it may never happen

- If all that happens is that only some of us deploy DNSSEC, then the entire DNSSEC effort is largely a waste of time, because of the trust point discovery problem in the current DNSSEC model

- Can we devise a more robust partial deployment model that can deliver benefits to both the DNSSEC signed zone publisher and the DNSSEC-aware resolver client base?
  - Is the DLV model of interest here?
  - Are there other approaches?

Another Opinion



Thank You