UKNOF16

Ralf Weber
(ralf.weber@nominum.com)

Who is Nominum?

Mission	Product Leadership	Industry Expertise
- ***Deliver the Trusted Internet Experience*** - ***Strategic Partners:*** YAHOO! EQUINIX Sun microsystems Qwest Global Crossing NTT Communications	- ***Best DNS Security*** - ***Highest Scalability*** - ***Highest Reliability*** - ***All Open Standards*** - ***Pioneered <u>Intelligent DNS</u>*** Enabling rules and policies for every DNS request to protect end-users and ensure they reach their intended destination	- ***Dr. Paul Mockapetris*** Inventor of DNS, IETF Chair: 1994-1996 Lifetime award: ACM SIGCOMM 2005 - ***Bob Halley*** Co-Architect of BIND8 Architect of BIND9 - ***Ted Lemon*** Developer of ISC-DHCP Co-author of DHCP Handbook - ***Over 30 Standards authored or co-authored***

Securing the Worlds' Largest Carriers DNS Infrastructure with Over 170M Broadband Households

BT
verizon
orange
NTT Communications
TELECOM ITALIA
COLT
comcast
Deutsche Telekom
Telefónica
Virgin media

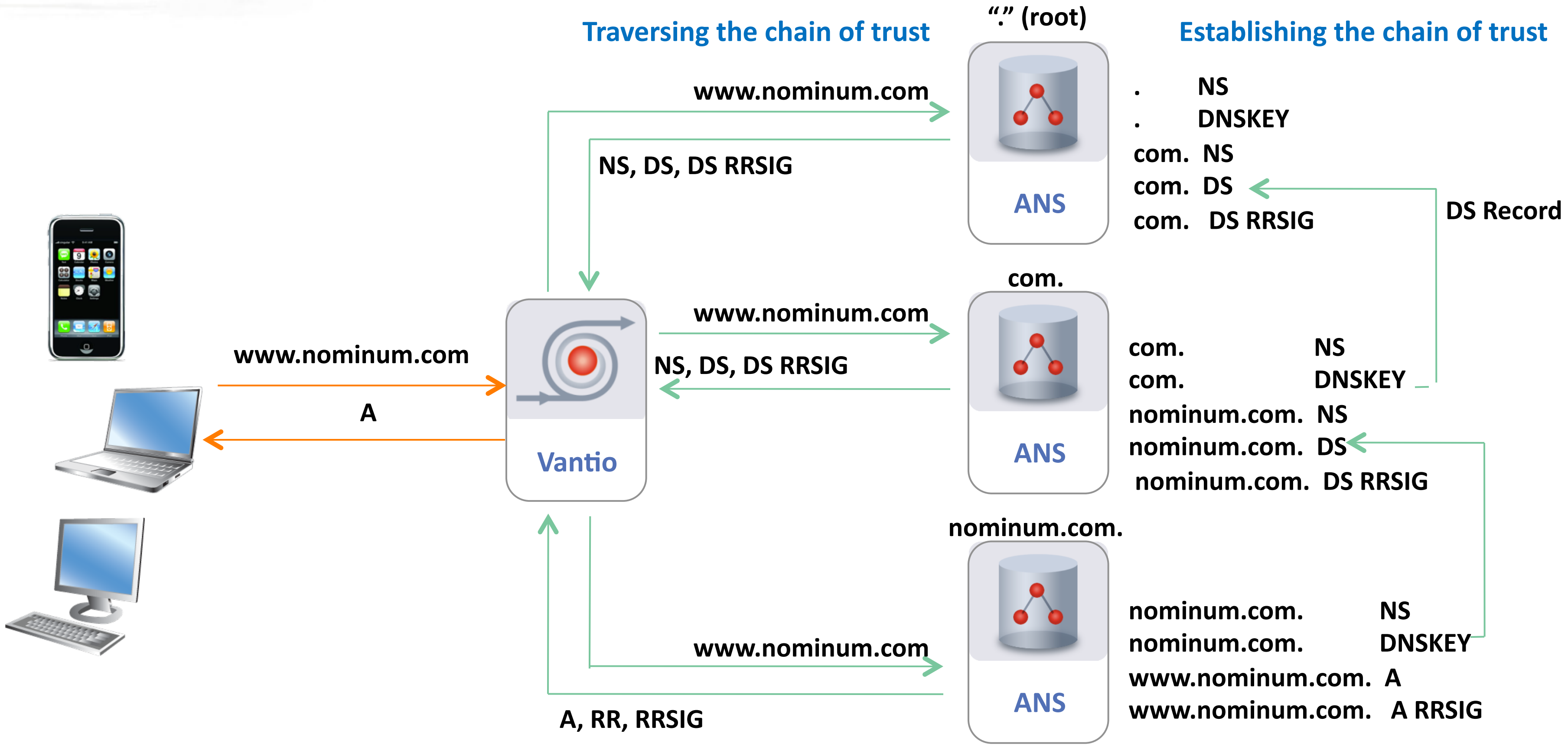
DNS is good

- It created a whole industry
- It scales in every direction
- It’s very hard to break
- It’s the central entry point into the internet
- Google has a DNS service so it must be cool
  - You might want to think about why they did this
- I love it so much I joined a company whose main business is DNS

DNS is bad (but there are solutions)

Problem	Solution
● Data Integrity	● DNSSEC
● Fast Flux Botnets	● Policy DNS
● Trojans (Conficker)	● Policy DNS
● Phishing (gøøgle.com)	● Policy DNS
● Cache poisoning (Kaminsky)	● DNSSEC
● Root Server Hijacking (China)	● DNSSEC

DNSSEC in one slide

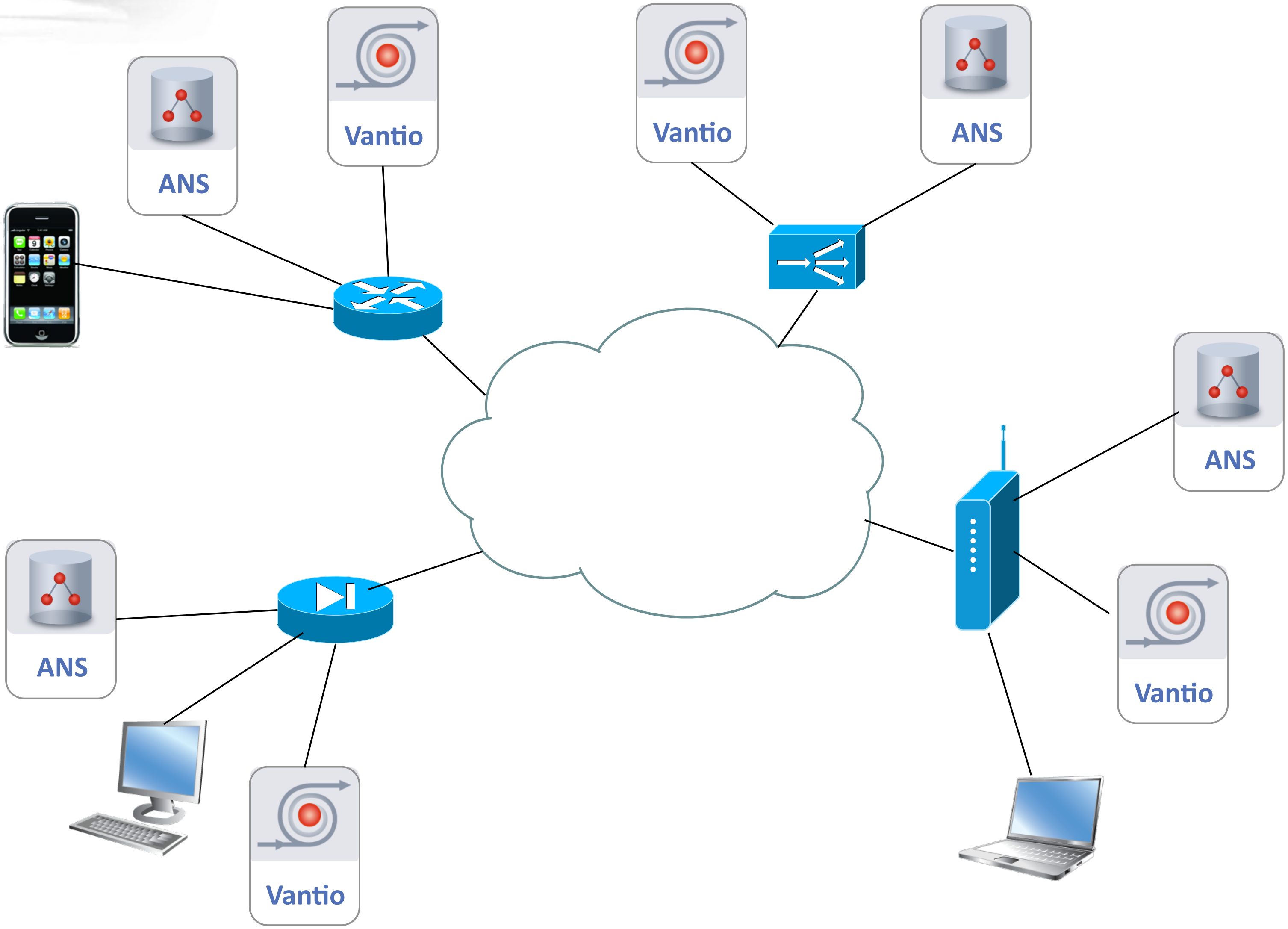


If verification is successful the DNS cache is populated with the A record, otherwise SERVFAIL is returned to clients

What can go wrong

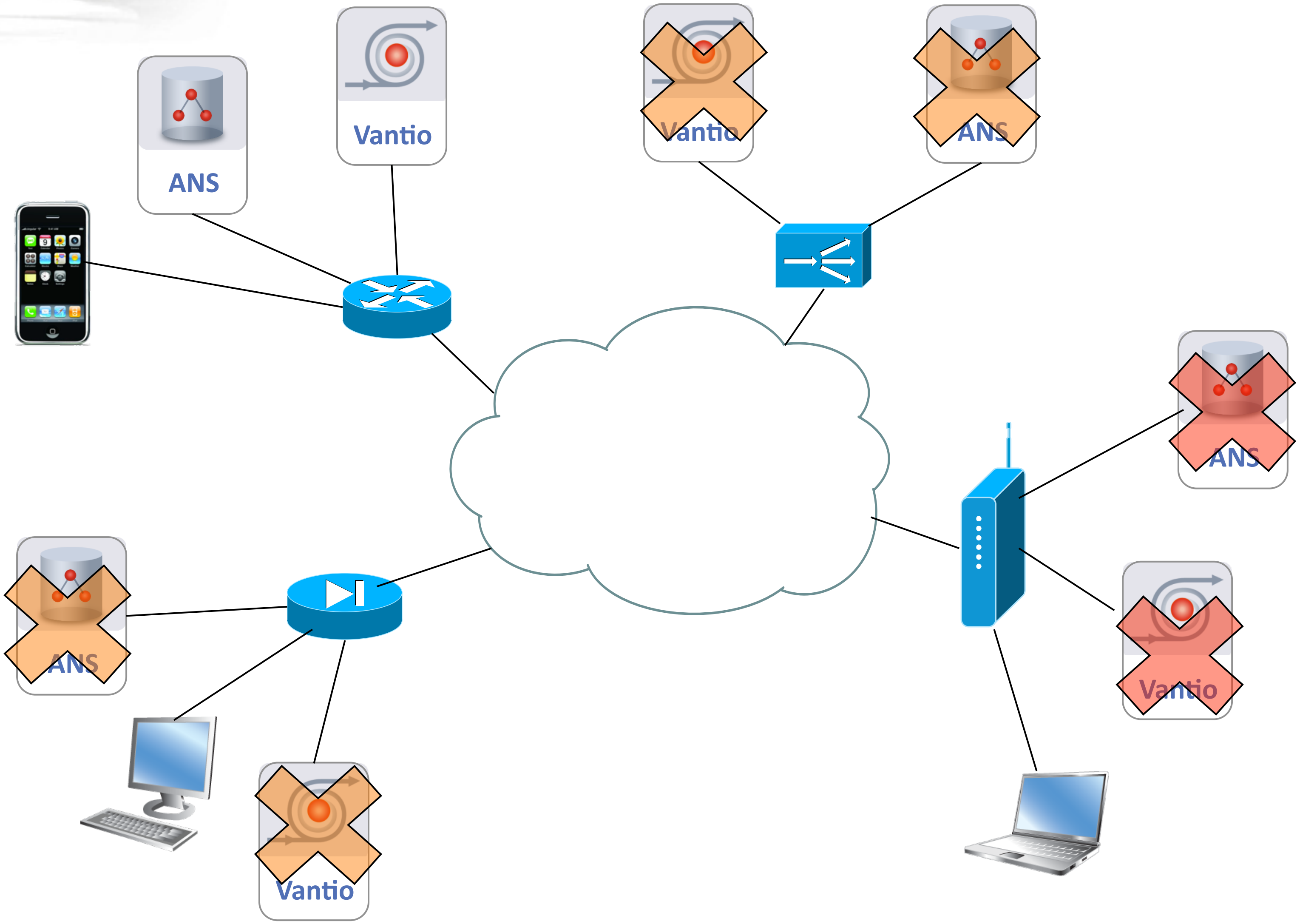
- Every error in the chain of trust disables it
- Cryptography requires constant changes
  - Signatures and keys have limited lifetimes
  - DNS data becomes dynamic with static content
  - Cryptographic algorithm may change
- Software has to be kept up to date or may fail
- DNS Data becomes bigger
  - A lot of people still believe DNS packets are 512 UDP only
  - DNS UDP packets can get up to 4096 bytes and fragment
  - If that’s not enough DNS will switch to TCP
  - Not all network devices might understand this

DNS and network devices



DNSSEC network problems

Nominum



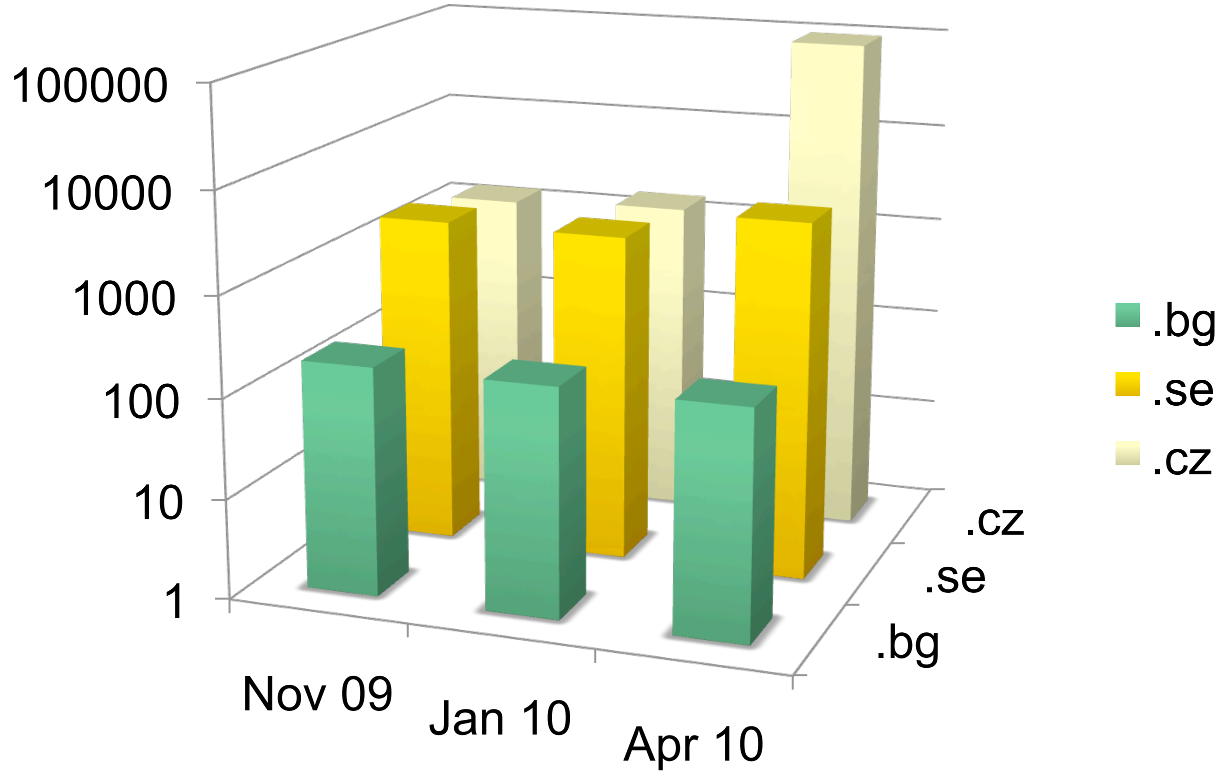
DNSSEC and the network

- Clients are fine
  - They don’t do DNSSEC validation at the moment
  - Windows and MacOSX don’t have a validator
  - Only Fedora has and they screw it
  - The home gateway (9 out of 38) discussion only affects geeks
- Don’t run DNS servers behind firewalls
  - It is possible but it usually requires configuration
  - Firewalls are not made for high qps throughput (to much state)
  - Enterprises that run a local bind resolver may have problems
- Load balancers should not alter DNS packets
  - Mostly applies for Global Server Load Balancing
  - You can use them for pure load distribution

Some DNSSEC statistics

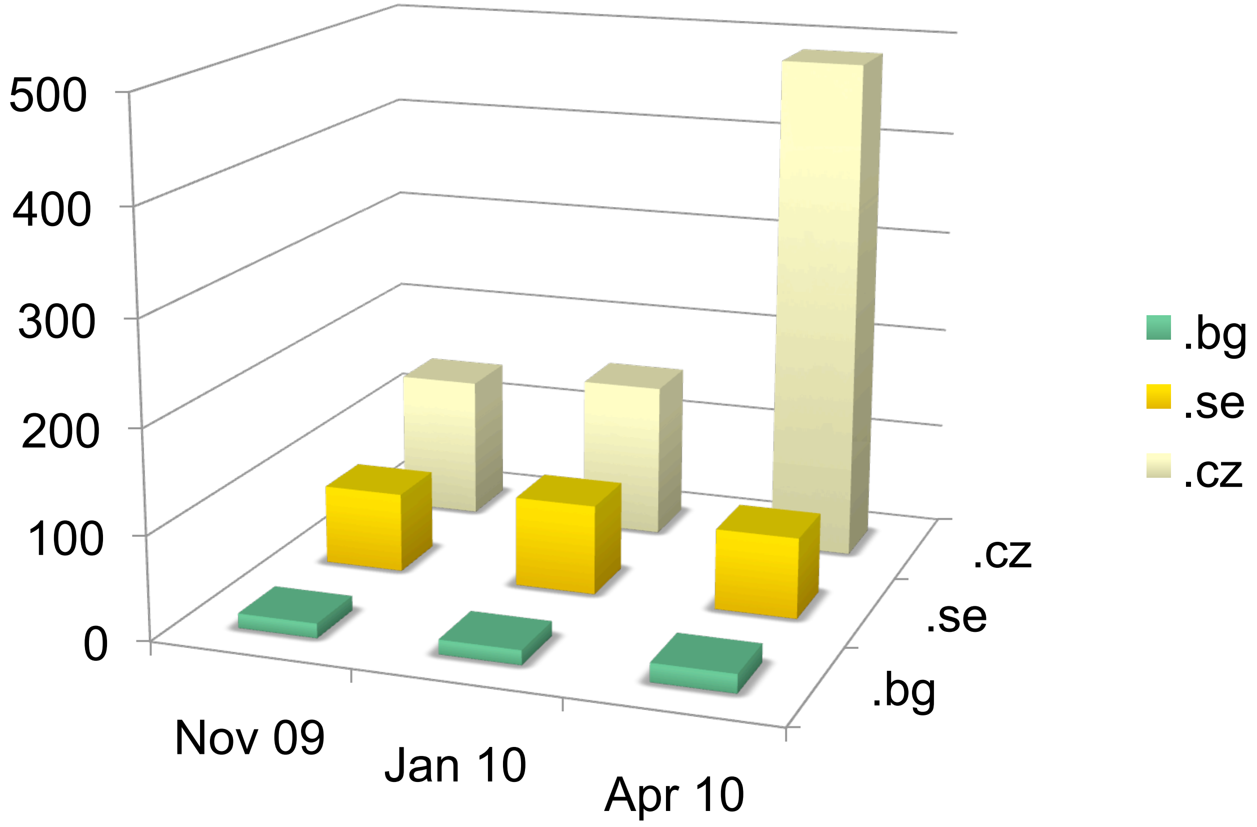
Nominum.

- Number of DNSSEC domains (log scale)



Some DNSSEC statistics

- Number of Domains that fail validation



Statistics Summary

- DNSSEC is gaining momentum
  - It’s good to see some large registrar taking it in CZ.
  - Some problems they might think about
    - All signatures expire at same time
    - Do not resign or roll everything at once
- Validation failures will be a problem
  - We need to get operators the tools to mitigate them
  - An insecure domain that resolves might be better than no resolving
  - Who would customers call when amazon.com failed

Validation failures

- How do validation failures happen ?
  - The data on the authoritative side is wrong
    - Signatures expired
    - New keys without DS delegation at parent
    - Domain owner doesn’t care about DNSSEC any longer (register.bg ;-)
- What can we do that they not happen ?
  - Don’t require 70 pages documents for people to setup DNSSEC
  - Make the operator interface the same as it used to be
  - Automate the resigning
  - Automate the key rollover
  - Automate the parent/child key relationship

Here’s how we do it

Insecure zone

```
@ 300 IN SOA  ( ns1 hostmaster
                1265702400
                3600
                600
                2592000
                300 )
@ 300 IN NS ns1
@ 300 IN NS ns2
ns1 300 IN A 192.0.2.1
ns2 300 IN A 192.0.2.2
www 300 IN A 192.0.2.3
```

Secure zone

```
@ 300 IN SOA  ( ns1 hostmaster
                1265702400
                3600
                600
                2592000
                300 )
@ 300 IN NS ns1
@ 300 IN NS ns2
ns1 300 IN A 192.0.2.1
ns2 300 IN A 192.0.2.2
www 300 IN A 192.0.2.3
```

Securing a zone

Nominum.

- One Server command
  - ans_dnssectool create-pack example.com
- What does it do
  - Generates Key and Zone signing key
  - Signs the zone (with RRSIG and NSEC)
  - When all is done this is an atomic update and the zone is served secure
- What happens then
  - Before the signatures expire the server will resign the zone
  - Once the zone is fully signed an atomic update will bring it live
  - When a zone signing key rollover is wanted at time X the server will pre publish the new keys so that the new signatures will be accepted
  - When a key signing key rollover is wanted at time Y the server will double sign the key set until the parent has change the DS

Example.com on the wire

Nominum.

```
example.com.            300     IN      SOA     ns1.example.com.
      hostmaster.example.com. 1265702401 3600 600 2592000 300
example.com.            300     IN      RRSIG   SOA 5 2 300
      20100427203428 20100420172928 2790 example.com. RMzVVs/
      uV227uAbY9bMsVBTpEEAU5AI8OA0lSQ82/S1E96AK15JKQPOF
      OaUuIUwGLPf3UMO63sK2cx5SjkbRl7tQyVRD6T2dpVoSlBi75+ys1eKV
      HqE5e0cVVSYS7SZWdlLcpLEZ/fjBYlwqakFIBdaIWiCis1Ebmls7VZy9
      r7M=
example.com.            300     IN      NS      ns1.example.com.
example.com.            300     IN      NS      ns2.example.com.
example.com.            300     IN      RRSIG   NS 5 2 300
      20100427203428 20100420172928 2790 example.com.
      Zxt7LBFIExK2a+HV7e+E+noft1JRQfnB0ZOydM1v84Q9sNOR9/ioZQ+3
      21hOirE92fYrPj6Qe5fHWH+3Ti1PwWz65+JnvokulBHk3OPn+au7/CUc
      Va20jLAZ47vs7GmDLURnBN1OU/pes1pSbqoqDAtFjwoUrmcGtCwUAqe8
      YkI=
example.com.            300     IN      NSEC    ns1.example.com.
      NS SOA RRSIG NSEC DNSKEY
example.com.            300     IN      RRSIG   NSEC 5 2 300
      20100427203428 20100420172928 2790 example.com.
      SVAmmyja6s1du6nn8eQkYbfinjiVFpJXeWsmkarq0qqVHbfU9mkhmAqJ
      tGehQXNxduhkCBbyntd4XlIOxXm6lUEvEB7SbseJIgwAUh0Pni95Q8rx YFM
      +hJ+Bh7dTxubzoo1f+Jyhtk3jGUHR1Dn9y+d3i4122pzYoHfvPlhP KKA=
example.com.            3600    IN      DNSKEY  257 3 5
      AwEAAaEIqFpfKtDclyTsxFkudKjAnKq6bBfAbEG8SrlrhN8tryRRqOdE
      cdpMSrEfmGpjJWbKZ9i39tjbYcZnwCHyM/GpR96VCZtSuZAePoHOvU+x
      9hG5qCG/Luy45shp3UFkVvURCqevYj6uj7ru5uHsAYZewwzcQoUvmVgl
      aiKxFE+j8tH0PJF/+5BNArBxWS1gKRxrjLVcuSwoPteHzZ6ZLCGsqao2
      ak5FK9B3QX1hIOQ64TgAbkDlGbWf8pyY3NoXk5vcJlnXyvABrfAbnfog
      V7xm44JGaET8LniMJhrLEFlVW6Z0a0ytHUOAiN2cYw0P/mLGqqu9OAGJ
      Cxuu3y07bmU=
example.com.            3600    IN      DNSKEY  256 3 5
      AwEAAdeD9EWc5olFuUhbW0xp06Zb3C+Lym+8UrpjAB0kdtSTeXr7v5Ww
      fFQFUu8bU6aC6lJFnAa2sPyZTHSjk+t71nQAAbn3ILsQxjVMQEIYemRX
      rBYMK+/qkoDJUs/excAbePoLnry6joEZ4muSamu8nAl2nxFhm8jQC9Vn
      3LugB0ez
example.com.            3600    IN      RRSIG   DNSKEY 5 2 3600
      20100427203428 20100420172928 2790 example.com.
      HnJGACrWQDEiphiZPtJ5q2Ar01glwe8znrkq9uhnM5wr+NDGzQz93utt
      1MGrd6P9b81VgeIbCGMoc7E1dKfDc9uch4/mzMkDhDDszSDVS5zke84n
      9ZCKnRiz/4pNLkLW32ktNgsMT5/oJ2UXla2gspTgohu/CQi4ZZdnXv2k
      6ZY=
example.com.            3600    IN      RRSIG   DNSKEY 5 2 3600
      20100818173428 20100420133428 13426 example.com. N
      +UsDZ8B04S51Y6Ujt/o+MQ5HtxdkRQEaCNEpoMq6WG0QEUvxmrCWAvH
      cG9x9P12D0gJz36AS53cnrcdgMn5BePt6D/EXIhprO9eBtK+zpHaoNcQ
      a3bjIkz3J3heGiVirZ2y5OeXCXLY4J0w86c8dRpgm5J0W0YXVe0rAExp
```

```
      RRSIG NSEC
ns1.example.com.        300     IN      RRSIG   NSEC 5 3 300
      20100427203428 20100420172928 2790 example.com.
      Q6VyE0WGs7jUN5qder4f9WpVG9oWsaJ2v07FPwmIxa9uwcefISX6QgMN
      HIBsRA2YPLYBobNeN9TFMmAVpHPerG5UD45DA4hO2JwLptiU56D2o5AN
      FsQoTt4WEQ7o1L70NsZ+NfdXj+C6oKTJYlzIQ7u2dH1e2f1Y/yDwwZyl
      C44=
ns2.example.com.        300     IN      A       192.0.2.2
ns2.example.com.        300     IN      RRSIG   A 5 3 300
      20100427203428 20100420172928 2790 example.com. BbEKmp2Lb/
      Mt9cZtkQ/4H5rZQpy9sTPrEYcfjSKqf324gSd5abwWK47+
      VY1WT2WWo2WWXCW1Ir6gJgR5MUuIrw1gEaW7iMHhHctIaAdkDT0Z3gJT
      Fbl7TqfpiaA2g+xl5d9GdgN3B7EnpLpHZ2asTAmbRoO7F40JrTt+pZ7o
      baI=
ns2.example.com.        300     IN      NSEC    www.example.com. A
      RRSIG NSEC
ns2.example.com.        300     IN      RRSIG   NSEC 5 3 300
      20100427203428 20100420172928 2790 example.com.
      MXC2zhyPkQAWPFaL9Y/bZ5U9wDC0goHLa6MEU5nYsEZTjBe52Txxo1j/
      kxBCuv0TUfeTvbLc194rtJOO7MWlxK1v1mI0B13Vr8v2D9lTrYAT4px1
      IlaV2clQ2NVmI0ERFZSWeEEti4iBfXg2bBuAq2s/vzlEZ5SMqJSSCDV4
      GXo=
www.example.com.        300     IN      A       192.0.2.3
www.example.com.        300     IN      RRSIG   A 5 3 300
      20100427203428 20100420172928 2790 example.com.
      vAKUvf6lrNCyzuvwdyFD0j5YEpvm+KX9/85BlvyeGVmimRvgCciZRXt5
      fBgKgS1+4tqZ7iF2GaHsxsyfuFr4e3+z++efNSvgJPujh4bGKJXXg1lo
      RQWL2HNlocKeyY7hGhSxPX1hP+so7GRd4fZ2UDazQ5wiC7sSTX7xrL9l
      soQ=
www.example.com.        300     IN      NSEC    example.com. A
      RRSIG NSEC
www.example.com.        300     IN      RRSIG   NSEC 5 3 300
      20100427203428 20100420172928 2790 example.com.
      JnYMUFvVMKxoU9XWI+wD13oSzLkeh7b5QB88n4SKSF4QGZRseTOmCjzq /
      ntiWM1vIs4E3zs09y5eVrhB3E8O0GgUxdcMI2PaUSN0J1pdfHkl++yt
      bZhqTjIis+2cgd0qtjQX4JuvkiU1IOMLBcijEri28JP6rR5McurfWwNU
      0x4=
```

Policy DNS

Nominum.

- A resolver is the first thing asked by most Internet applications
- If we know that the questions is bad we can protect the user
  - Not allowing trojans to download their payload
  - Notify the User if he or she e.g. is infected with malwar
  - Don’t let Users go to phishing sites
- Governments in Europe also use this to protect their citizen
- If you know what the user asked does not exist you can guide him if you want

The future

- DNSSEC will come and we fully support and automate it
- Our customers do
  - Comcast announced that it will fully support DNSSEC in 2011
  - Enable DNSSEC in all caching resolvers
  - Will sign all their 5000 zones
  - All be done using our products
- You should too
  - ISPs/Telcos should start to run DNSSEC validating resolvers
  - Sign your zones

Thank You!

- Q & A!