Exceed Together

DNS: The good, the bad and the ugly

Ralf Weber (rw@colt.net)

The good

- DNS is a success story
- DNS created a whole industry
  - you can make money on two or less letters ;-)
- It scales in every direction
  - some people now even want to use it for RFID
  - biggest distributed database out there and in your Intranet
- It’s used beyond it’s initial usage (name to number conversion)
  - ENUM
  - Service discovery
  - Security/Spam protection
  - RFID

The bad

- DNS wasn't designed with security in mind
- Cache poisoning was a problem since the early 1990s
  - People believed to have that fixed with QID (16 bit)
  - Some didn't understand randomness (CA-1997-22, CVE-2007-2926)
  - Some got it right and used 32 bits from the start (including Daniel J. Bernstein)
- Last year Kaminsky discovered a new way to poison cache
  - 1.colt.net, 2.colt.net, 3.colt.net.....
  - Suddenly 16 bit were not enough
  - We increased to 32 bit, but will this be enough for tomorrows networks
- A solution to DNS security problems does exist.....

The ugly (DNSSEC)

- Let’s be clear DNSSEC will come
  - The rocket has been lit (we have a date for a signed root)
  - We don’t know yet what orbit it will reach
- Current problem statement
  - DNSSEC will protect against cache poisoning
  - DNSSEC is per Domain (~ 180 Million of them out there)
  - Protecting servers (~ 3 Million out there) would be easier
  - Daniel J. Bernstein was correct again (DNSCurve), but no market share

DNSSEC until now

- Development should be finished now
  - it is the third try of the IETF so should be ok
  - no so sure when reading namedroppers
  - software and tools are not all up to the latest spec
- Big change in operation of DNS service
  - DNS was very hard to break, and easy to setup (Install and forget)
  - DNSEC will stop working soon if you not constantly manage it
    - Security always goes against convenience (signature lifetime)
    - A lot of it could be automated but....
    - The current tools/software for DNSSEC all suck (only Nominum seems to have some promising stuff coming soon)

DNSSEC deployment

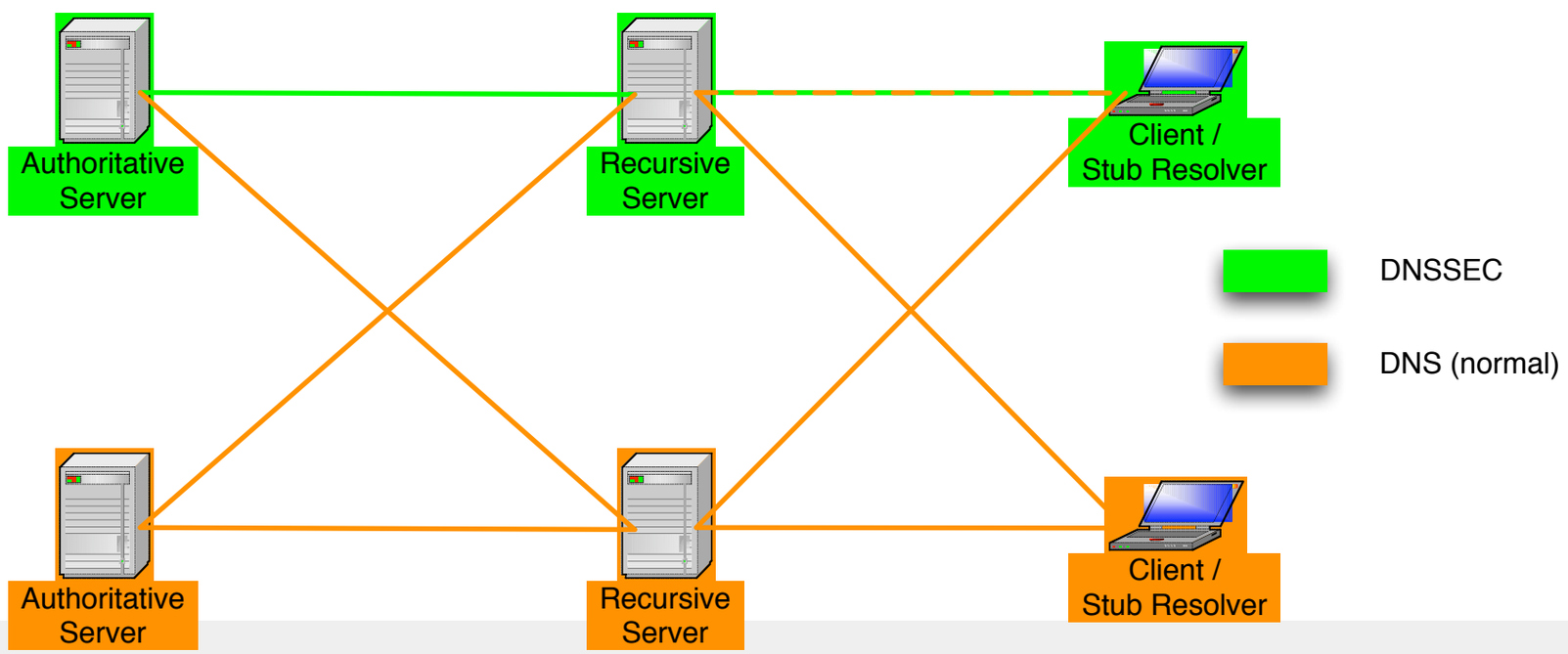
- .se, .br, .cz,... some TLDs have already done that
- signing your zone without having a mechanism to delegate securely (DS records) is not DNSSEC deployment for TLDs
  - .org and others will still tell you so
  - doing this only increases traffic, but not security as NS records are not signed
- DNS provider changes still are a big unknown with DNSSEC
  - I’ve heard of one secure transfer in sweden
  - .org is working on it (shouldn’t they work on something else ;-)
  - .de currently has ~100.000 transfers/provider changes per month
- Some scaling IMHO has not been thought of
  - Most of the current early adopters have a limited number of zones to care about
  - What about signing several million of small zones
- It will be a bumpy road

DNS Redirect

- I am co-author of draft-livingood-dns-redirect which describes how DNS server shall handle that
- I first encountered the problem when Colt was obliged by law in 2005 to do that in Italy to stop the Italian people to gamble online
- Since then adoption has increased as well as other usages
  - 7 countries in the EU do it (only 3 have DNSSEC deployed at the moment)
  - some others have voluntary redirects
  - some providers do NXDOMAIN redirects in order to guide users to websites
  - can protect against malware, trojans, phishing (e.g Conficker)
- There can be some bad usages (e.g censorship), but the technology in itself isn't bad
- Can it work with DNSSEC?

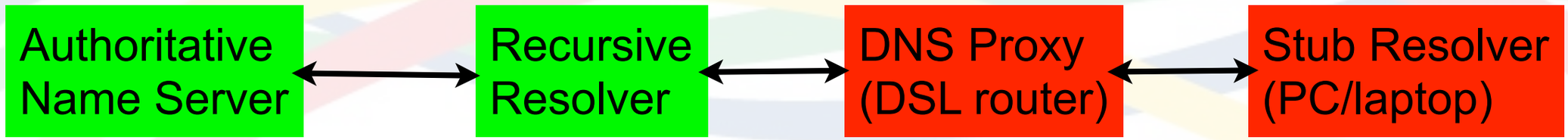
DNS Redirect and SEC

- Non validated answers will not be used/sent
  - for secured domains that have been properly delegated and have trust anchors
- If you want to block access that's what you want anyway
- Only redirection will not work
- If the system giving out the redirection also is the system validating then even this will work when there is further validation
- Let's see how is validating what:



The end to end myth

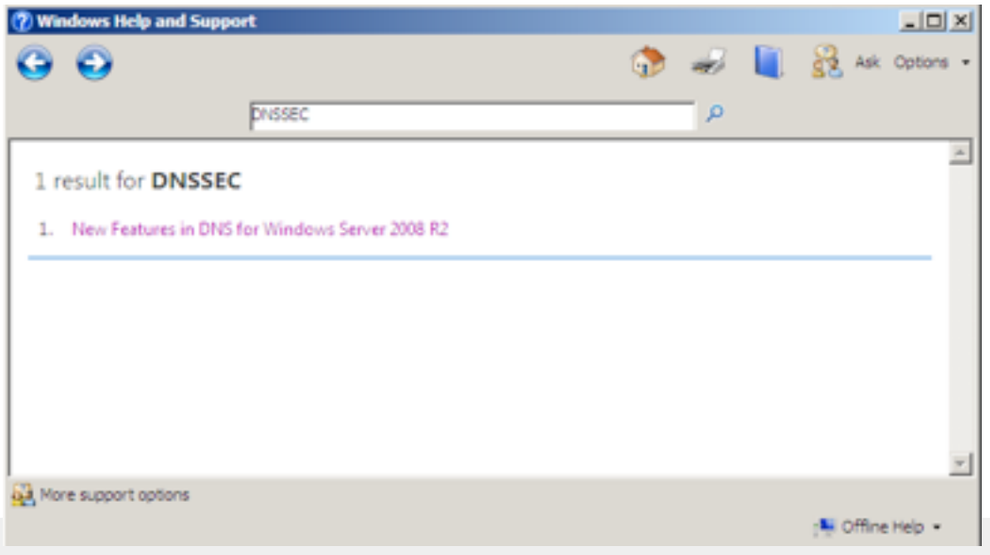
- DNSSEC was designed to protect the authenticity of the data from the zone owner to the end system requesting it (PC, laptop, etc)
- What actually is communicating (colors indicate DNSSEC support)



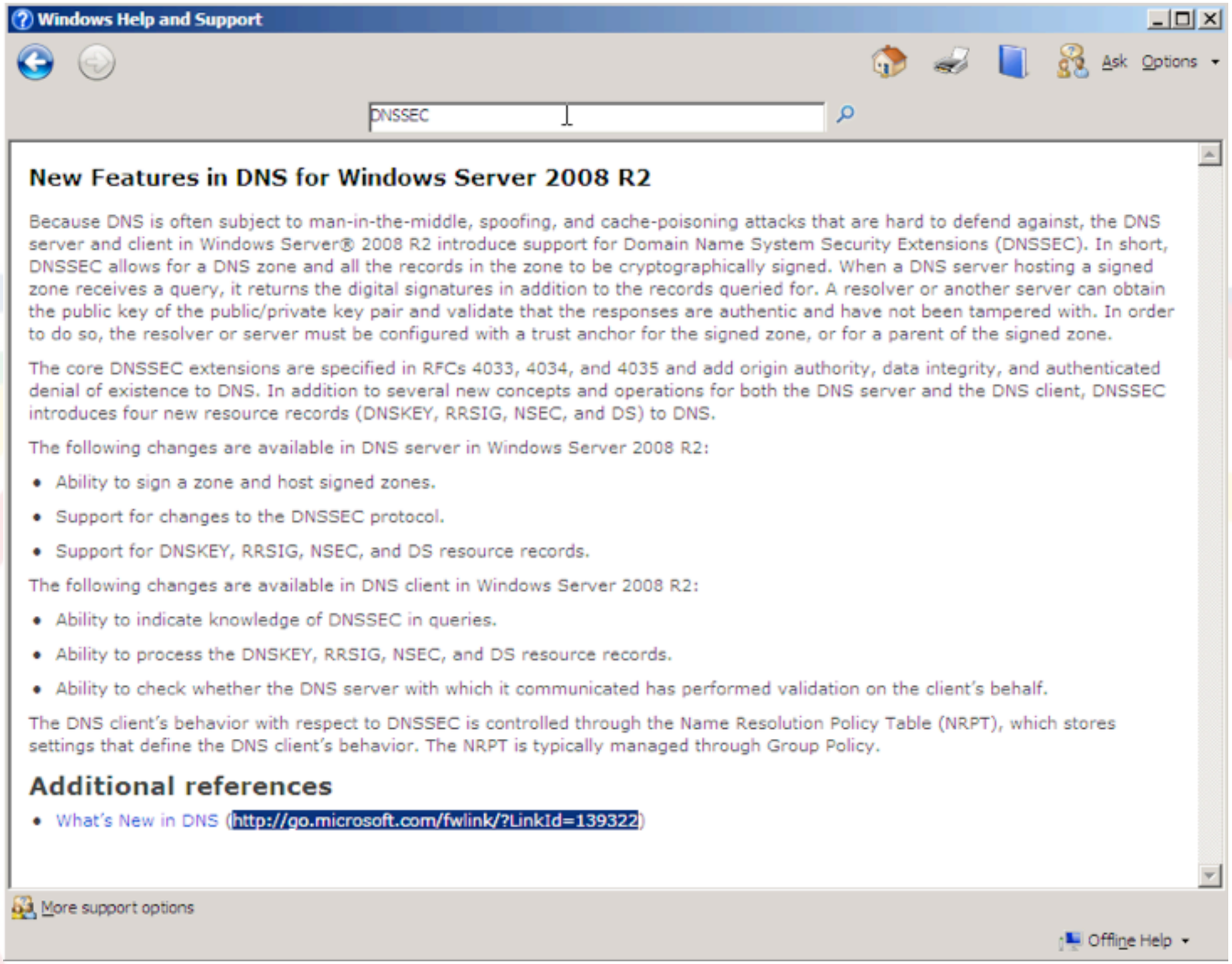
- As long as DSL routers are having problem proxying DNSSEC request as an OS vendor I wouldn't enable DNSSEC
  - only 25% can proxy DNSSEC out of the box (http://download.nominet.org.uk/dnssec-cpe/DNSSEC-CPE-Report.pdf)
- There is one OS offering DNSSEC support out of the box
  - Fedora
  - Other Unixes including Mac OSX could configure it
- But wait didn't Windows recently gained DNSSEC support?

The Windows has DNSSEC myth

- I did stop using Windows at home in 2001
  - So I welcome comments from Windows admins
  - I think my DNSSEC findings are accurate though
  - Thanks to MS for providing trial software
  - All tests where done on Windows Server 2008R2
  - DNSSEC Client support should be identical in Windows 7
- After installing Windows Server 2008R2 I did a search for DNSSEC:



Windows and DNSSEC continued



Windows and DNSSEC continued

- That is all the info on DNSSEC that Microsoft provides on the system
- The link gives the same content
- If you search long enough there is one document though
  - http://www.microsoft.com/downloads/details.aspx?FamilyID=7a005a14-f740-4689-8c43-9952b5c3d36f&DisplayLang=en
- Some initial findings for authoritative zones on reading it
  - DNSSEC zones can not live in AD and can not receive dynamic updates
  - You have to work with textfiles and command line (No GUI support)
  - The actual process of getting to a secure zone is 8 pages with lot's of dnscmd command lines with lots of options. Example:
    - DnsCmd /OfflineSign /SignZone /input <input zone file> /output <output zone file> /zone <zone name> /signkey /cert /friendlyname ksk1-<zone name> /signkey /cert /friendlyname zsk1-<zone name> /signkey /cert /friendlyname zsk2-<zone name>

Windows and DNSSEC continued (Recursive Resolver)

- Windows 2008R2 has a recursive resolver
  - Resolver can do validation
  - You can configure multiple trust anchors
  - No NSEC3 (RFC5155) support
  - No SHA256 (RFC4509/RFC5702) support
- The Resolver does work as expected, but
  - with all new TLDs using NSEC3
  - root will be signed with SHA256
- In the current state the resolver is not usable

Windows and DNSSEC continued (DNSSEC Client)

- Windows now has a: Non-validating security-aware stub resolver
- What the heck is this
  - Well first and foremost it doesn't perform validation
  - It simply examines the content of the AD bit (of course bad guys will not fake that ;-)
  - To make sure that this is not faked MS want's you to do an IPSEC Tunnel to the resolver (which is something providers love to do for free ;-)
  - AD Examination can be set on domain or TLD level
  - If you do a TLD e.g *.se everything below it has to be secured
  - By doing the above you have denied access to 99.78% of swedish domains
- Conclusion: The Windows DNS Client even with only AD bit examination is not usable in normal Internet usage
- Final conclusion: Windows does some DNSSEC, but it is not usable

Some DNSSEC statistics

- I did walks of some signed TLDs at the beginning of November 2009
- .se has 0.22% of it's domains signed (1957)
- out of these 4% have validation failures (77)
- 1638 DNSSEC domains belong to four big registrars without errors
- .cz has 0.22% of it's domains signed (1340)
- out of these 10% have validation failures (137)
- the biggest registrar has 1000 DNSSEC domains
- .bg has ~1% of it's domains signed (192)
- out of the 7% have validation failures (14)
- the biggest registrar has 174 DNSSEC domains
- register.bg does not validate ;-)

DNS Crystal Ball

- After looking at the above my predictions are:
- DNSSEC adaption initially will be slow
  - It will kick of when the mass providers offer it as standard
  - Secure transfers have to work
  - **Better, easy to use software and tools are desperately needed**
- ISPs and TLD operators have to make sure that validation works
  - Validation has to be monitored or it will be turned of soon
- Clients will not do validation in the near future
- Legal authorities will demand more DNS redirection
- ISP will use this technology to do other things
  - protect customers
  - guide customers (and maybe make money)

Thank you

Questions ?