DNSSEC

Your Internet infrastructure needs better protection

Matthijs Mekking, ISC

Matthijs, ISC

- Working on DNS and DNSSEC for 18 years
  - NLnet Labs (research, dev)
  - OpenDNSSEC (dev)
  - Dyn (DNS provider)
  - ISC (dev BIND 9)
  - IETF (standards)

What is DNSSEC

What is DNSSEC

- Digital signatures on RRsets
- Hierarchical PKI
  - End-to-end integrity
  - Origin authentication
- A set of IETF specifications
  - RFC 4033 4034 4035, and more
- Backwards compatible with DNS

Why DNSSEC

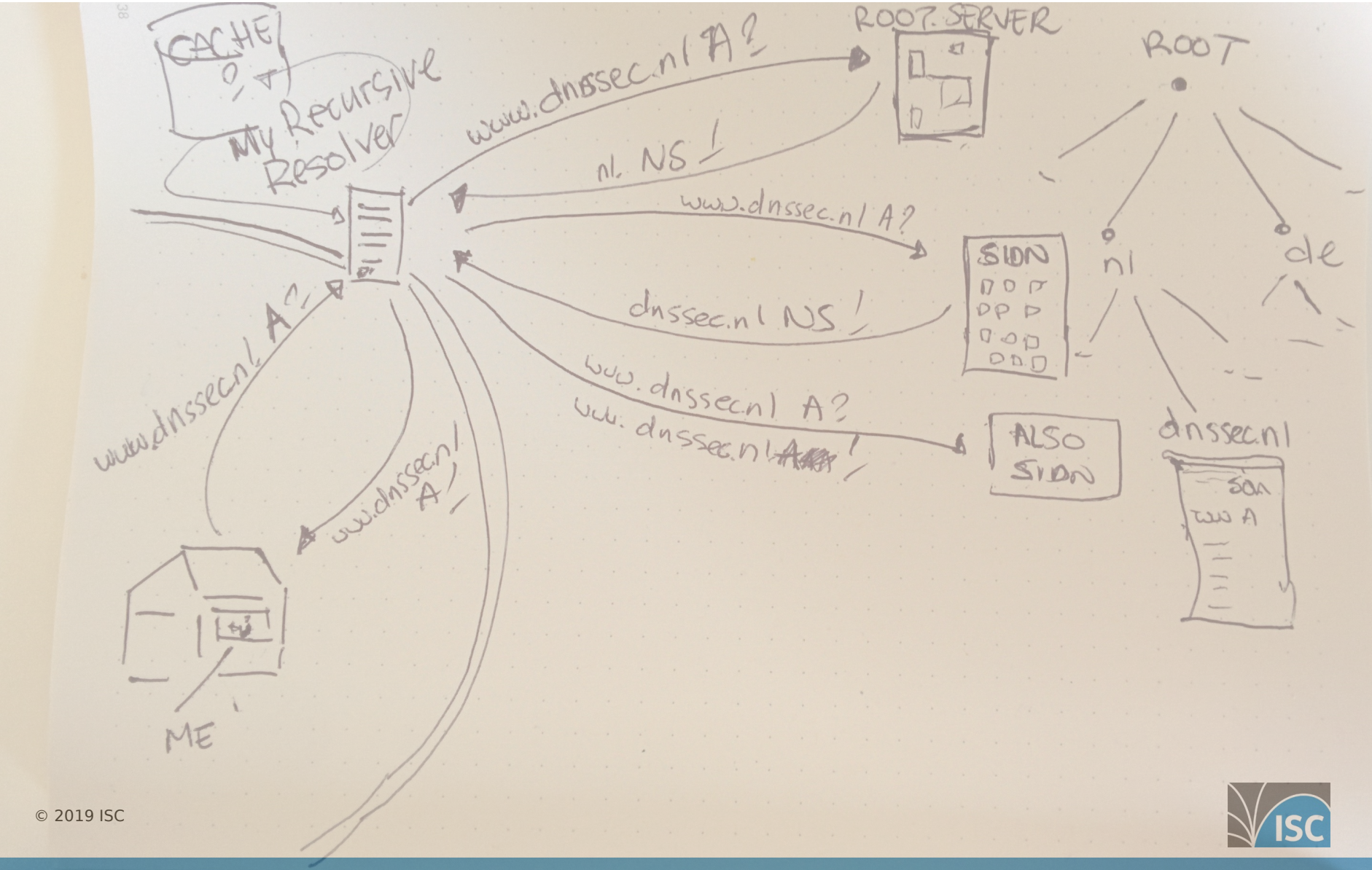
- Prevent cache poisoning
  - Data integrity and authentication
- Bootstrap other security systems
  - DANE: TLSA
  - IPSECKEY
  - SSHFP

What DNSSEC doesn’t do

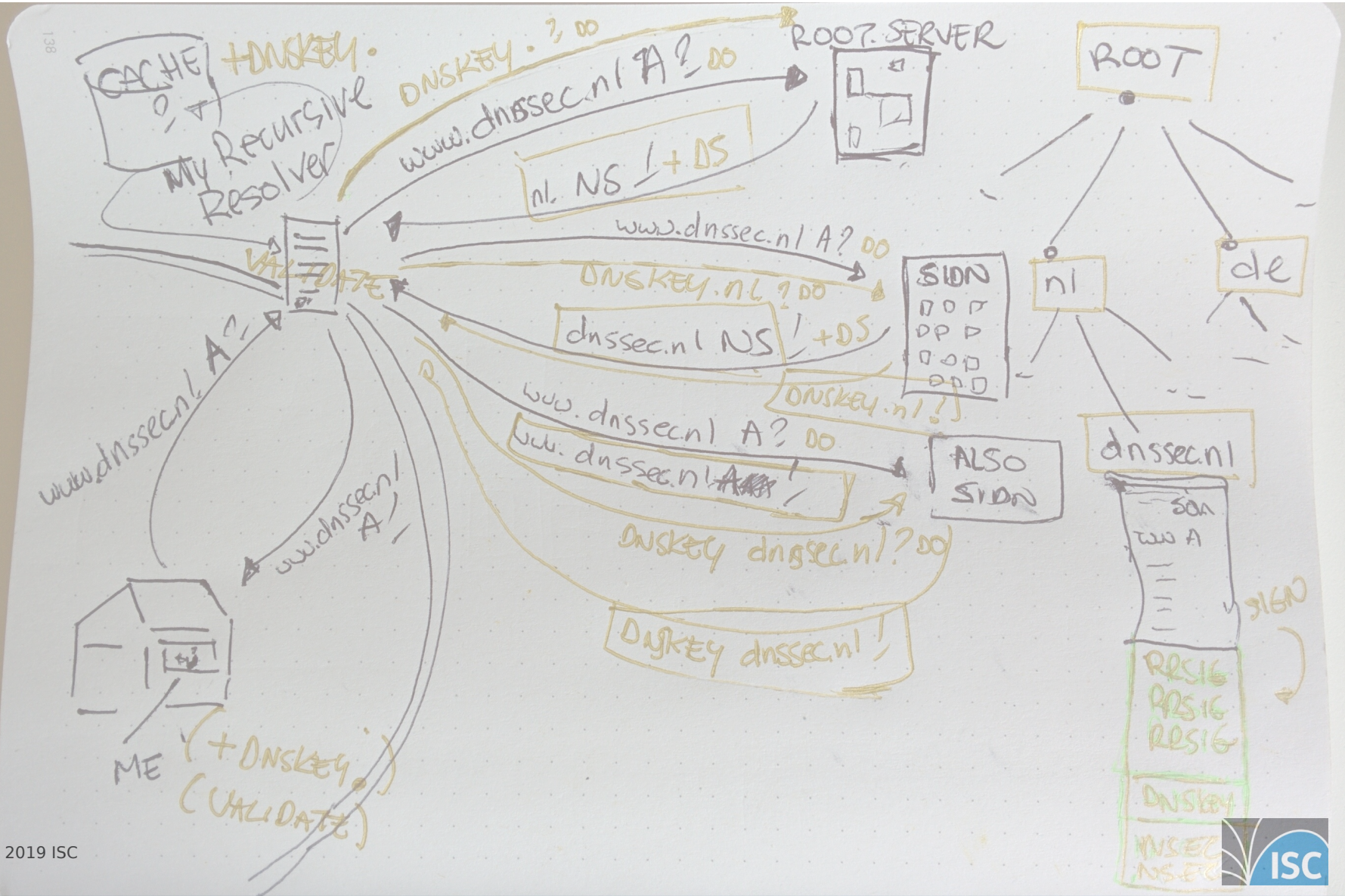
- Privacy/confidentiality
- DDoS protection
- Message security
- Access control

Not a silver bullet,
but a building block for a more secure Internet infrastructure

How DNSSEC works

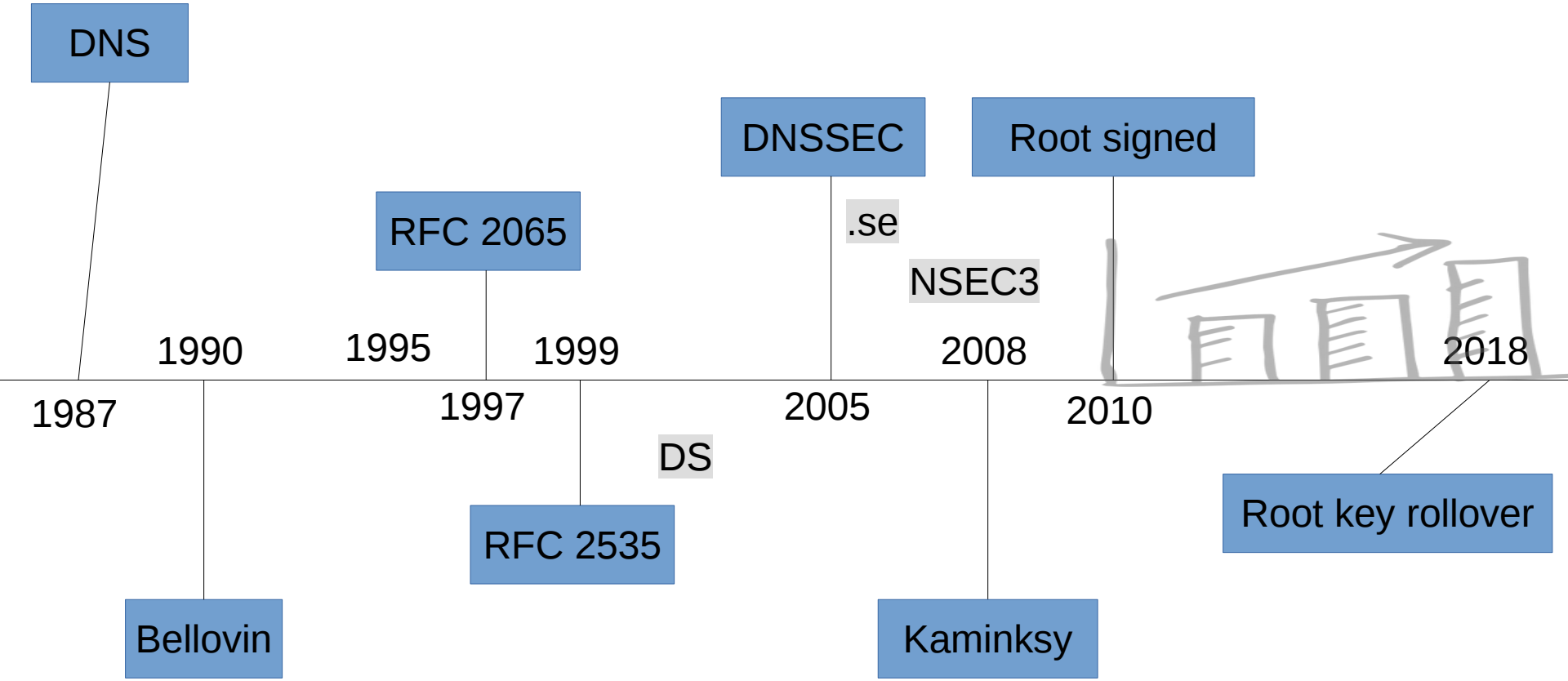


How DNSSEC works



Status of DNSSEC

History of DNSSEC



Deployment status

- Signing:
  - Root, 91% tld
  - 3% Fortune 1000
- Validation:
  - ~20% (APNIC)
  - Includes Google, CloudFlare

.no	58%
.se	54%
.nl	53%
.ch	4%
.com	0.7%

Deployment challenges

- Perceived complexity of DNSSEC
  - Long standardization process
  - Early adopter DNSSEC errors highlighted
- Wide variety of many DNS systems
- Root DNSSEC key ownership
  - Trusted Community Representatives
- The incentive problem
  - “All work and no play makes Jack a dull boy”
  - The costs outweigh the benefit

DNSSEC Weaknesses

- RFC 3833 (2004)
  - Complex to implement
  - Increased work load
  - The last mile
  - Increased DNS response size
- Weak error signaling (SERVFAIL)

Arguments used against DNSSEC

- DNSSEC is complex
- It is computational heavy
- DNS poisoning risk is low
- Root key owners control the DNS
- The last mile is insecure
- There are better alternatives
- SERVFAIL: Bad error signaling
- DNSSEC means amplification attacks
- The costs outweigh the benefit

Debunking arguments against DNSSEC


DNSSEC
its just so hard...

It’s not

DNSSEC Software

- Signing:
  - BIND 9, Knot DNS, PowerDNS, OpenDNSSEC (+appliances, closed)
- Validating:
  - BIND 9, Unbound, Knot Resolver, PowerDNS (+appliances, closed)

DNSSEC Software

- Push the button config, one page docs
- Many config options for corner cases
  - Soft validation
  - Negative trust anchors
- Auto resign, ZSK management
- Tools for making KSK rollover easier
  - Requires DS update in parent zone
  - Not required for normal operation
- Provide support contracts

More work load

The cost of validation

- More computational resources
- More DNS queries (DNSKEY, DS)
  - Up to 5x more queries with no cache
  - Up to 4x slower with no cache
  - Implementation dependent
- But...

The cost of validation

- Caching helps a lot
  - Equal number of queries and time

Cache poisoning risk low

The threat is real

- Kaminsky attack
  - Made cache poisoning trivial
  - Source port randomization made it 65536 times harder
  - But that is just patch work

New DNS Attacks Make Use of DNSSEC More Critical Than Ever

By: Wayne Rash | February 26, 2019

NEWS ANALYSIS: A series of nation-state attacks on DNS networks pose a threat to both government and enterprise computing networks and mean that immediate action may be necessary.

WEBINAR: On-Demand

Desktop-as-a-Service Designed for Any Cloud ? Nutanix Frame

An insidious new series of cyber-attack traffic intended for specific websites DNS records has resulted in the fir by the Cybersecurity and Infrastr This directive was followed in ICANN (Internet Corporation Numbers) of a growing eff attackers to compromis through attacks on to

What this means to change your orga

ICANN warns of "ongoing and significant" attacks against internet's DNS infrastructure

Zack Whittaker @zackwhittaker / 1 month ago

Comment

SWITCH

SWITCH Security Blog

DNSSEC Usage in Switzerland is on the rise after widespread attacks on the Domain Name System

02/04/2019 by Michael Hausding | 1 Comment

Attacks on the DNS System

Cyber attacks on the DNS system are not new. Cache poisoning, Domain Hijacking and BGP injections of

Science 26 Feb 2019

Core internet infrastructure plagued by 'multifaceted' attacks: Details here

Written By Shubham Sharma

The Internet Corporation for Assigned Names and Numbers, which is the organization responsible for managing internet addresses, claims the core infrastructure of the internet is under attack.

ICANN has issued a warning noting that the key parts of the DNS infrastructure are at risk of attacks and have to be protected with a new technique.

Here's more on this issue and ICANN's potential solution.

You May Also Like

SC asks states to ensure safety of Kashmiri

Jaish leadership eliminated within 100 hours of Pulwama

#Pulwama: Stop blaming Pakistan and China, Chinese media

Elders of the Internet

TCRs

- Trusted Community Representatives:
  - Recognized members of the DNS technical community from various regions to perform key management
- Goal:
  - Improve confidence and acceptance in the DNSSEC security mechanism among the wider Internet community

Resolver to client

Resolver to client

- Validation at the client
  - DNSSEC-Trigger
  - getdns API for applications
- Securing the transport
  - DNS over TLS (DoT), DNS over HTTPS (DoH)

Alternative solutions

Alternatives to DNSSEC

- Channel security mechanisms
  - DNSCurve
  - DNSCrypt
  - DNS over TLS (DoT)
  - DNS over HTTP (DoH)
  - Hop-by-hop authentication

Alternatives to DNSSEC

There is no real alternative for
providing data integrity
and origin authentication

SERVFAIL

DNS Extended Errors

Amplification attacks

Amplification

- This is also possible without DNSSEC
- Mitigations:
  - Refuse ANY
  - Enable minimal responses
  - DNSSEC Combined Signing Key

Amplification

- RSA 1024 bit: ~132 bytes DNSKEY
- RSA 2048 bit: ~260 bytes DNSKEY
- ECDSA:
  - ECC P-256 bit: ~100 bytes DNSKEY
  - Equally strong to RSA 3100 bit
  - Towards 512 bit DNSSEC responses
  - Much faster signing
  - But slower validation

To conclude

Costs versus benefit

- DNSSEC has become a lot better
  - More mature software
  - Protocol improvements
- Rise of DNS attacks
- Financial incentive programs

DNSSEC Call for Adoption

- Protect your Internet infrastructure
  - Prevent cache poisoning
  - Data integrity, origin authentication
- Bootstrap other security systems
  - TLSA, SSHFP, IPSECKEY, ...
- Easy deployment
  - Software matured, push the button
- Some protocol weaknesses exist
  - But improvements are on the way!

Links

- **Information and sources**
  - **IETF:** https://www.ietf.org
    - DNSSEC RFCs: https://tools.ietf.org/html/rfc4033 https://tools.ietf.org/html/rfc4034 https://tools.ietf.org/html/rfc4035 https://tools.ietf.org/html/rfc5155
    - Elliptic Curve Digital Signature Algorithm (DSA) for DNSSEC https://tools.ietf.org/html/rfc6605
    - Extended DNS Errors: https://datatracker.ietf.org/doc/draft-ietf-dnsop-extended-error/
    - DNS over TLS: https://tools.ietf.org/html/rfc7858
    - DNS over HTTPS: https://tools.ietf.org/html/rfc8484
  - **IANA:**
    - **Trusted Community Representatives:** https://www.iana.org/dnssec/tcrs
  - **Deploy360**: https://www.internetsociety.org/deploy360/dnssec/ https://www.dnssec-deployment.org/
  - **APNIC Measurements:** https://labs.apnic.net/
  - **OpenINTEL:** https://openintel.nl/
  - **The Cost of DNSSEC:** https://www.potaroo.net/ispcol/2014-08/dnsseccost.pdf
- **Software**
  - **ISC (BIND 9):** https://www.isc.org/
  - **NLnet Labs (Unbound, OpenDNSSEC, DNSSEC-Trigger):** https://nlnetlabs.nl/ https://www.opendnssec.org/
  - **getdns:** https://getdnsapi.net/
  - **CZ.NIC (Knot DNS, Knot Resolver):** https://www.knot-dns.cz/ https://www.knot-resolver.cz/
  - **Open-Xchange (PowerDNS):** https://www.powerdns.com/
- **News**
  - **ICANN Calls for Full DNSSEC Deployment, Promotes Community Collaboration to Protect the Internet**
    - https://www.icann.org/news/announcement-2019-02-22-en
  - **DNSSEC Usage in Switzerland is on the rise after widespread attacks on the Domain Name System**
    - https://securityblog.switch.ch/2019/04/02/dnssecinswitzerland2019/

DNSSEC Panel

- Raise your questions and concerns!
- How can we make things easier?