DNSSEC

How it works

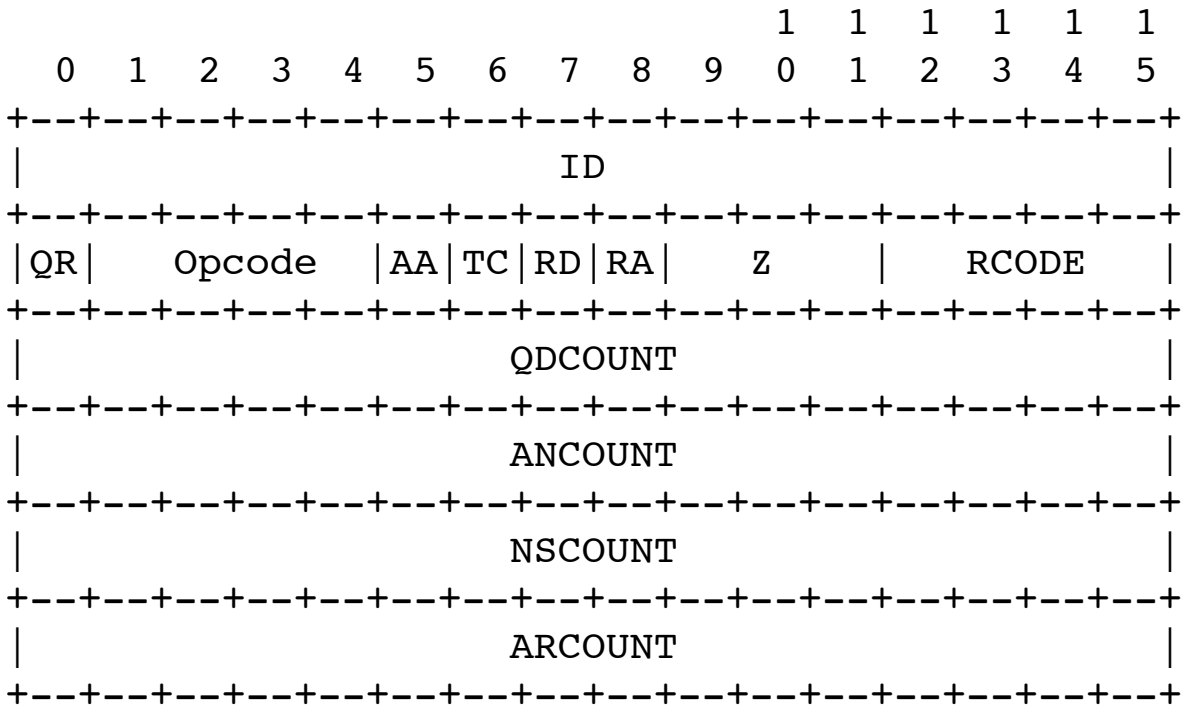
and

Why you really, really, need it

jay@nzrs.net.nz

Blame the ID field

RFC1035, section 4.1.1, DNS Header section format



Attack Vectors

Man In the Middle

Spoofing (guessing the ID)

jay@nzrs.net.nz

Great Firewall of China

Posted by Mauricio Vergara Ereche from NIC.CL on 25 March 2010: "A local ISP has told us that there's some strange behavior with at least one node in i.root-servers.net (traceroute shows mostly China). It seems that when you ask A records for facebook, youtube or twitter, you get an IP and not the referral for .com"

```
; <<>> DiG 9.6.1-P3 <<>> @i.root-servers.net www.facebook.com A
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7448
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.facebook.com.              IN      A

;; ANSWER SECTION:
www.facebook.com.       86400   IN      A       8.7.198.45

;; Query time: 444 msec
;; SERVER: 192.36.148.17#53(192.36.148.17)
;; WHEN: Wed Mar 24 14:21:54 2010
;; MSG SIZE  rcvd: 66
```

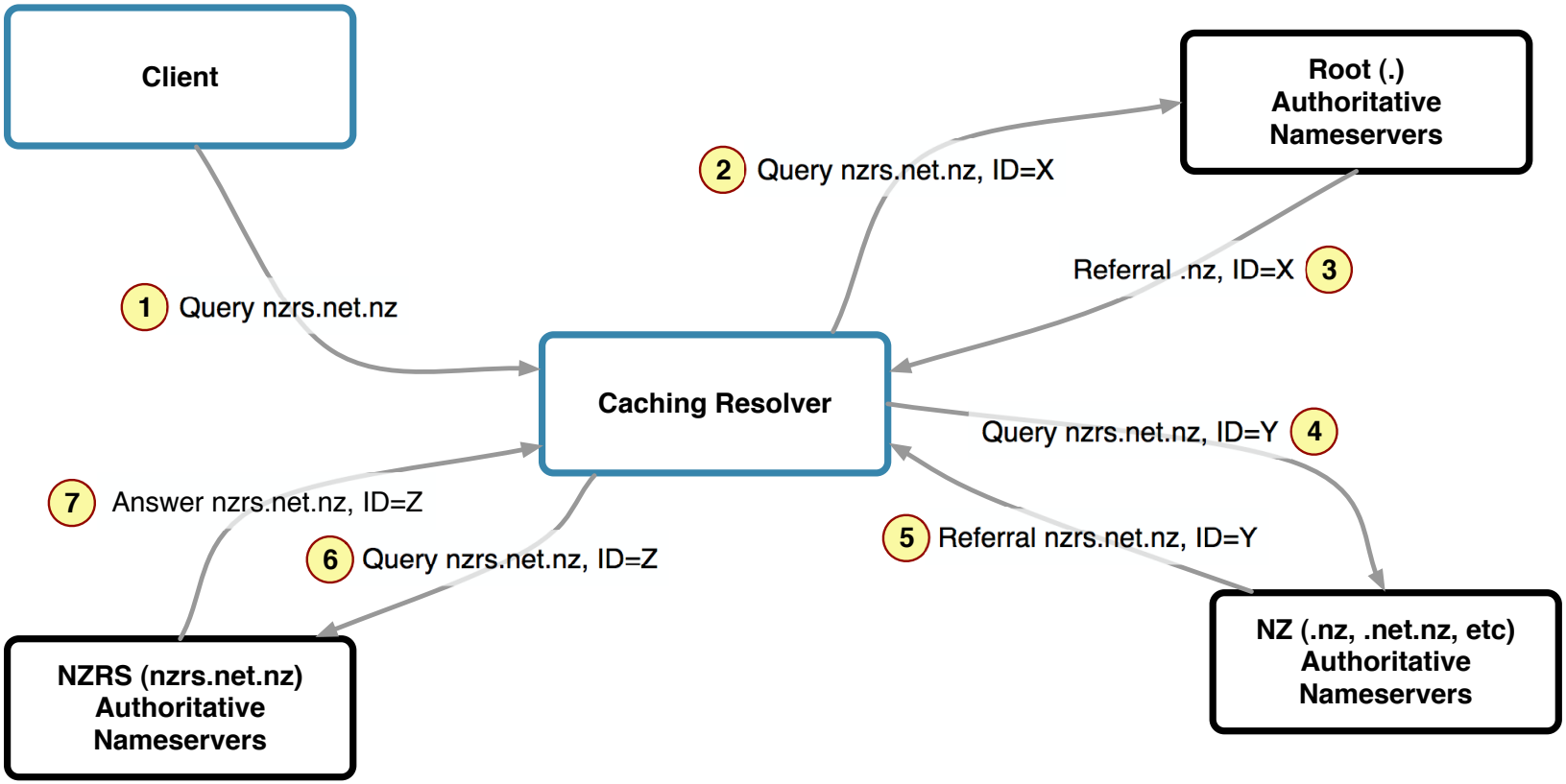
Great Firewall of China

Censorship in 5 easy steps

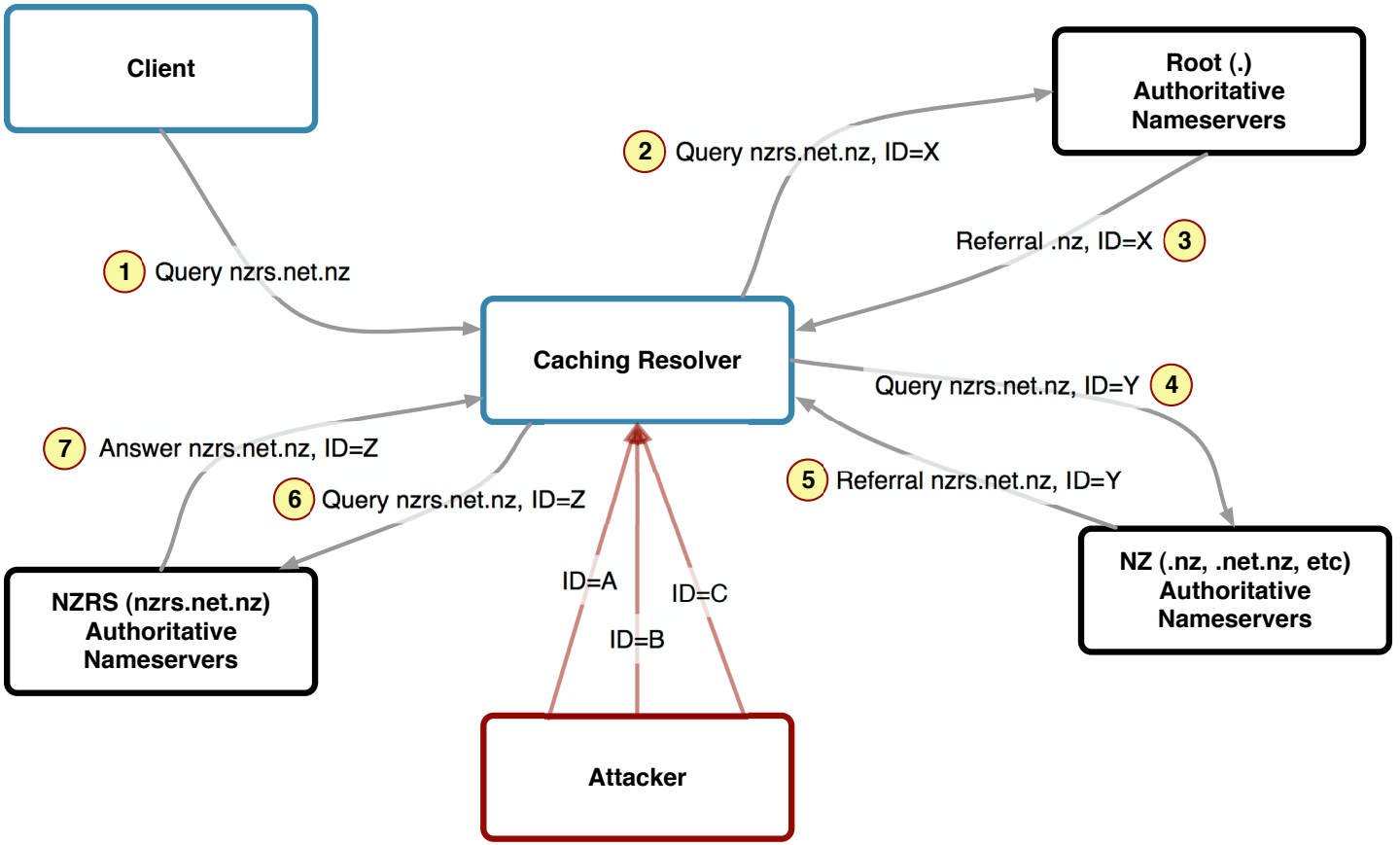
1. Send a DNS request to any Chinese IP address
2. Include partial string to be censored (twitter, facebook, youtube, and loads more)
3. Get a fake response from 80% of networks!
4. Redirected to non-existent IP address instead of correct referral
5. Censored until cache times out response TTL

jay@nzrs.net.nz

Normal resolution



Spoofing


Client
Root (.)
Authoritative
Nameservers
2 Query nzrs.net.nz, ID=X
1 Query nzrs.net.nz
Referral .nz, ID=X 3
Caching Resolver
Query nzrs.net.nz, ID=Y 4
7 Answer nzrs.net.nz, ID=Z
6 Query nzrs.net.nz, ID=Z
5 Referral nzrs.net.nz, ID=Y
NZRS (nzrs.net.nz)
Authoritative
Nameservers
NZ (.nz, .net.nz, etc)
Authoritative
Nameservers
ID=A
ID=C
ID=B
Attacker

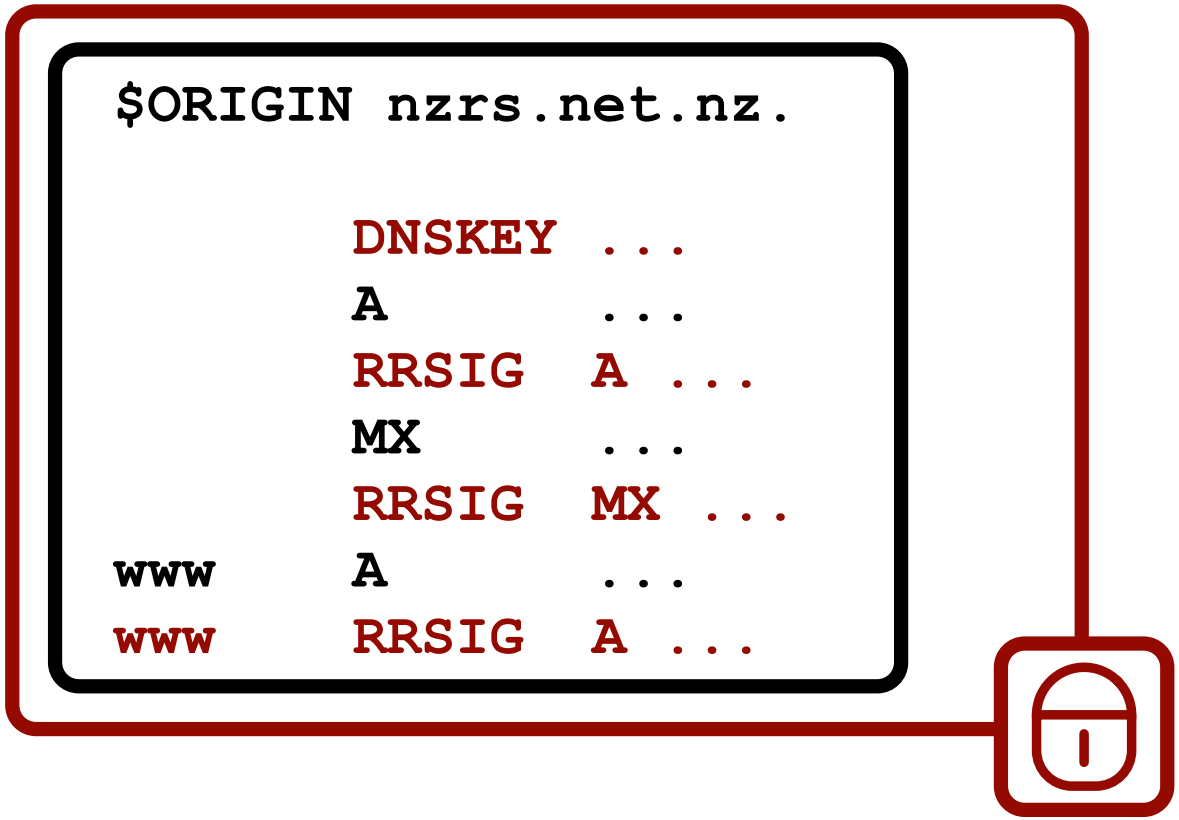
DNSSEC to the rescue

- Signatures on Authoritative responses
  - Including NXDOMAIN (domain does not exist)
- Does two things only:
  - Anti-spoof
  - Anti-tamper
- Does NOT do
  - Secure queries
  - Secure channel

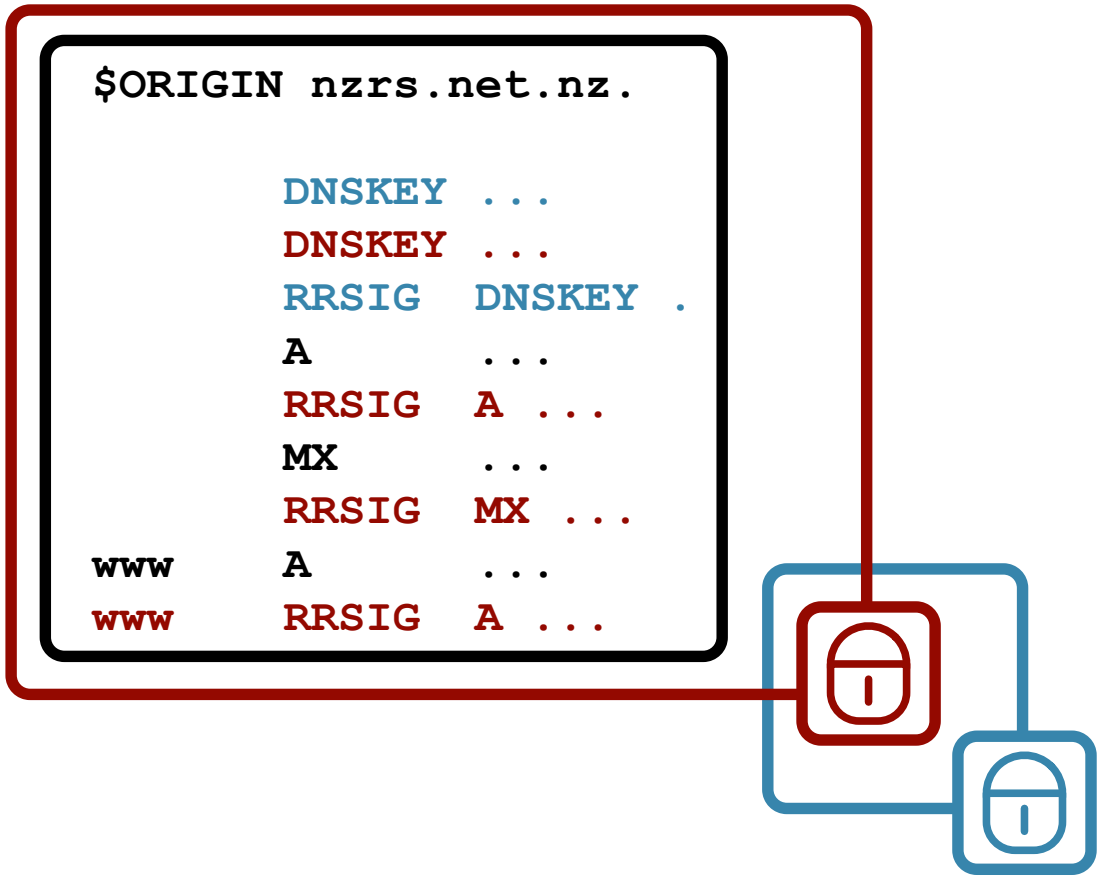
How it works

```
$ORIGIN nzrs.net.nz.

        A       ...
        MX      ...
www     A       ...
```

How it works


$ORIGIN nzrs.net.nz.
DNSKEY ...
A ...
RRSIG A ...
MX ...
RRSIG MX ...
www A ...
www RRSIG A ...

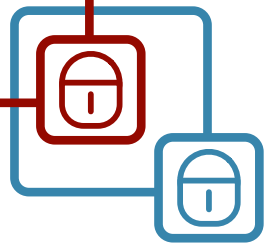
How it works


$ORIGIN nzrs.net.nz.
DNSKEY ...
DNSKEY ...
RRSIG DNSKEY .
A ...
RRSIG A ...
MX ...
RRSIG MX ...
www A ...
www RRSIG A ...

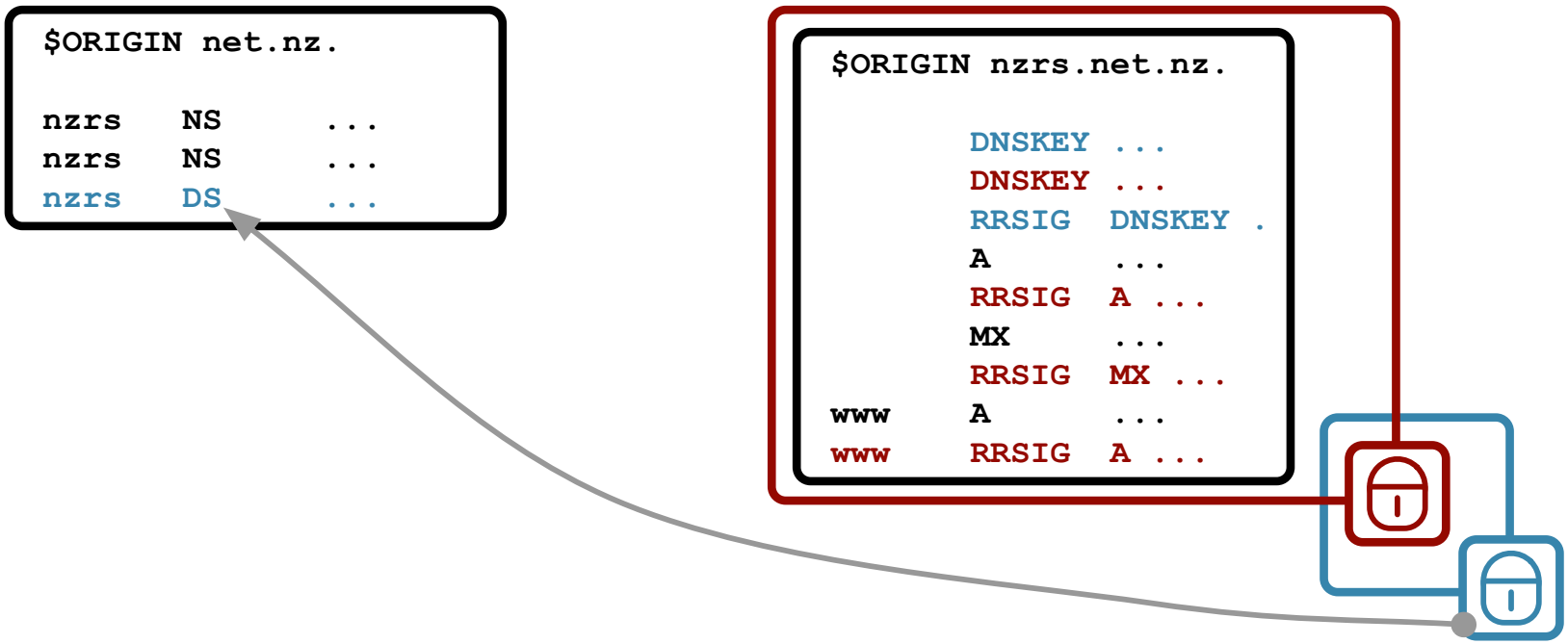
How it works

```
$ORIGIN net.nz.

nzrs    NS      ...
nzrs    NS      ...
```

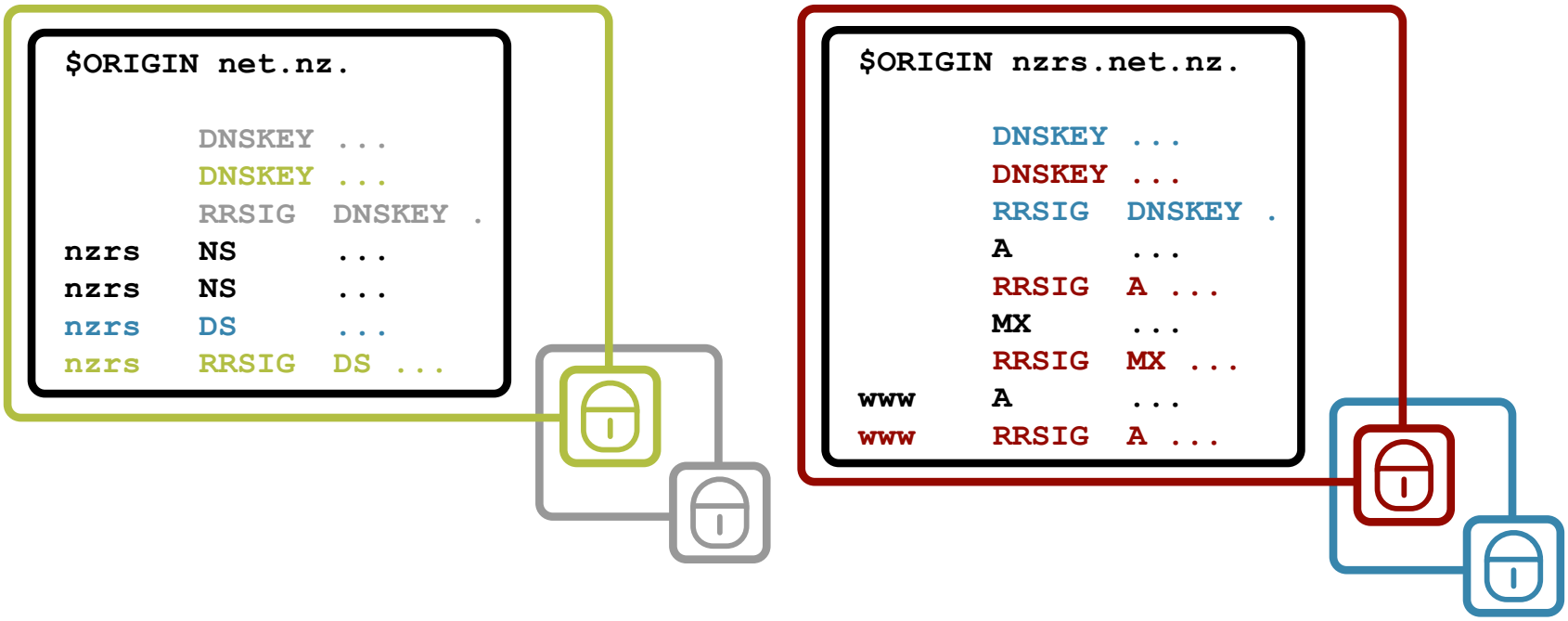
```
$ORIGIN nzrs.net.nz.

        DNSKEY  ...
        DNSKEY  ...
        RRSIG   DNSKEY  .
        A       ...
        RRSIG   A ...
        MX      ...
        RRSIG   MX ...
www     A       ...
www     RRSIG   A ...
```



How it works


$ORIGIN net.nz.
nzrs NS ...
nzrs NS ...
nzrs DS ...
$ORIGIN nzrs.net.nz.
DNSKEY ...
DNSKEY ...
RRSIG DNSKEY .
A ...
RRSIG A ...
MX ...
RRSIG MX ...
www A ...
www RRSIG A ...

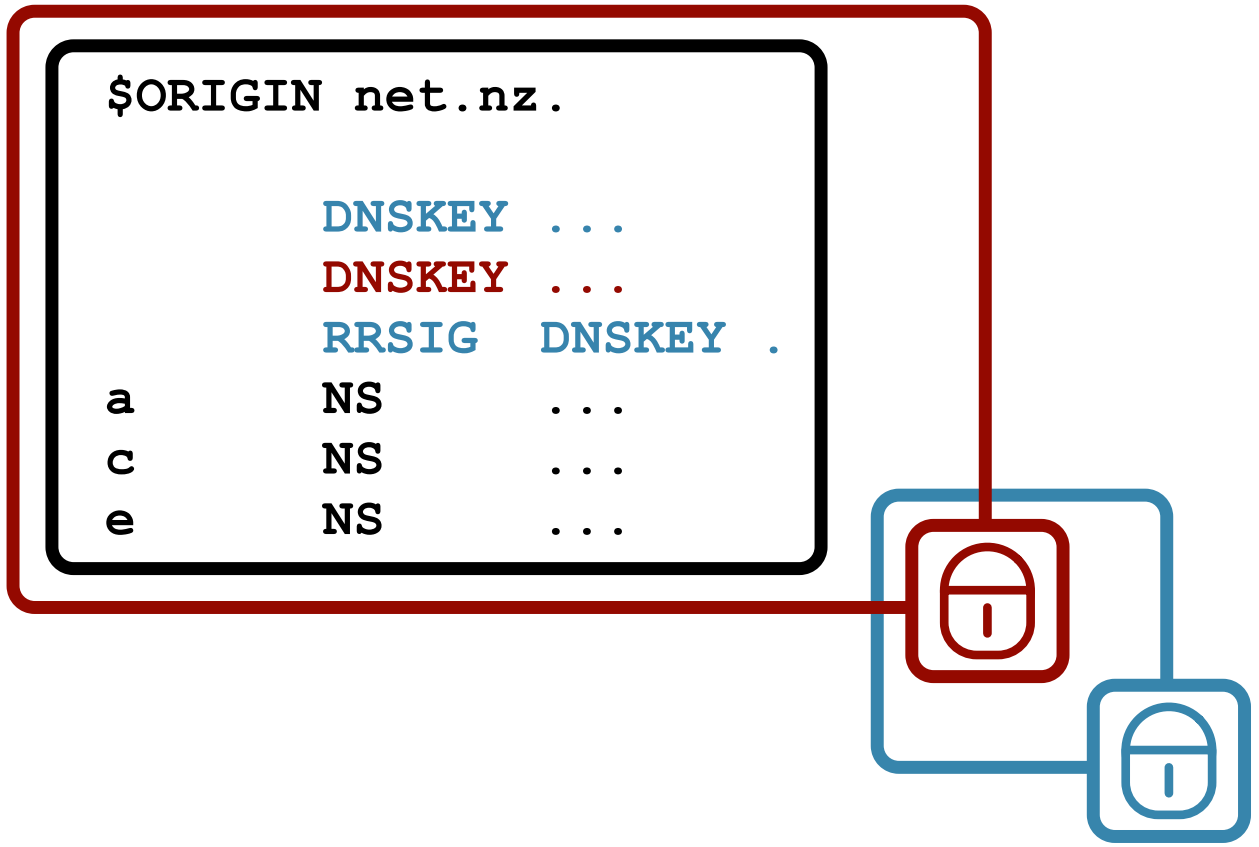
How it works


$ORIGIN net.nz.
DNSKEY ...
DNSKEY ...
RRSIG DNSKEY .
nzrs NS ...
nzrs NS ...
nzrs DS ...
nzrs RRSIG DS ...
$ORIGIN nzrs.net.nz.
DNSKEY ...
DNSKEY ...
RRSIG DNSKEY .
A ...
RRSIG A ...
MX ...
RRSIG MX ...
www A ...
www RRSIG A ...

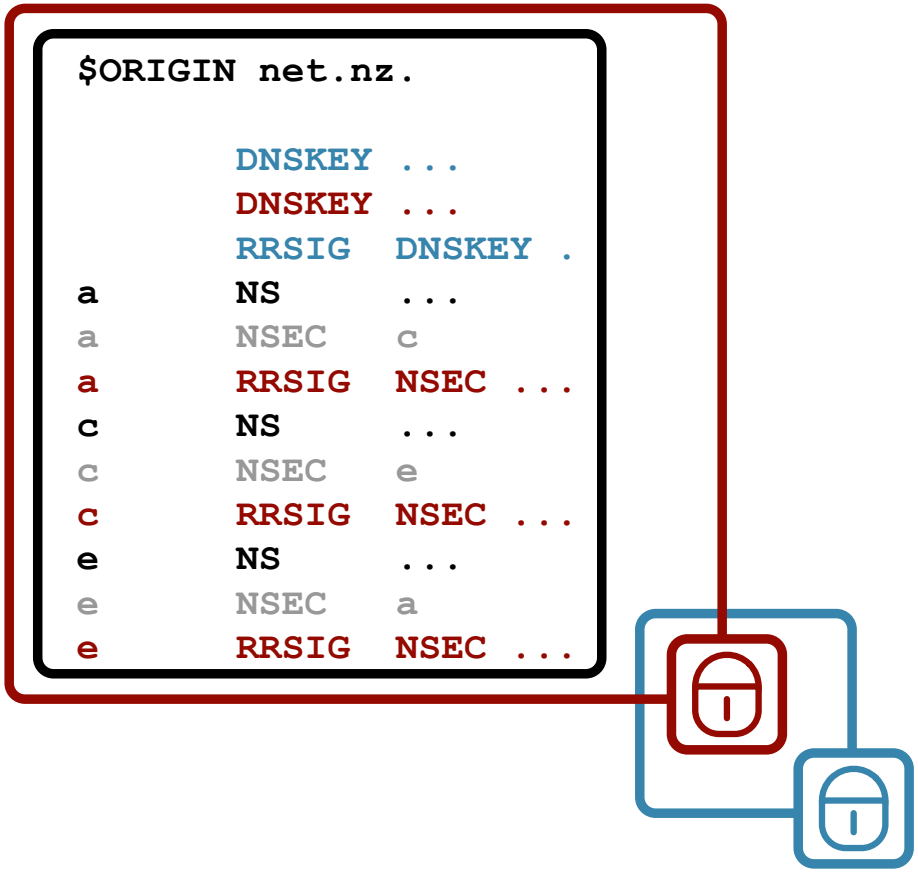
Recap

- Two types of keys
  - Zone Signing Key (ZSK)
  - Key Signing Key (KSK)
- New DNS Resource Records
  - DNSKEY : the keys used for DNSSEC
  - RRSIG : signatures over a set of resource records
  - DS : Delegated signer, hash of key at lower level

Authenticated denial of existence

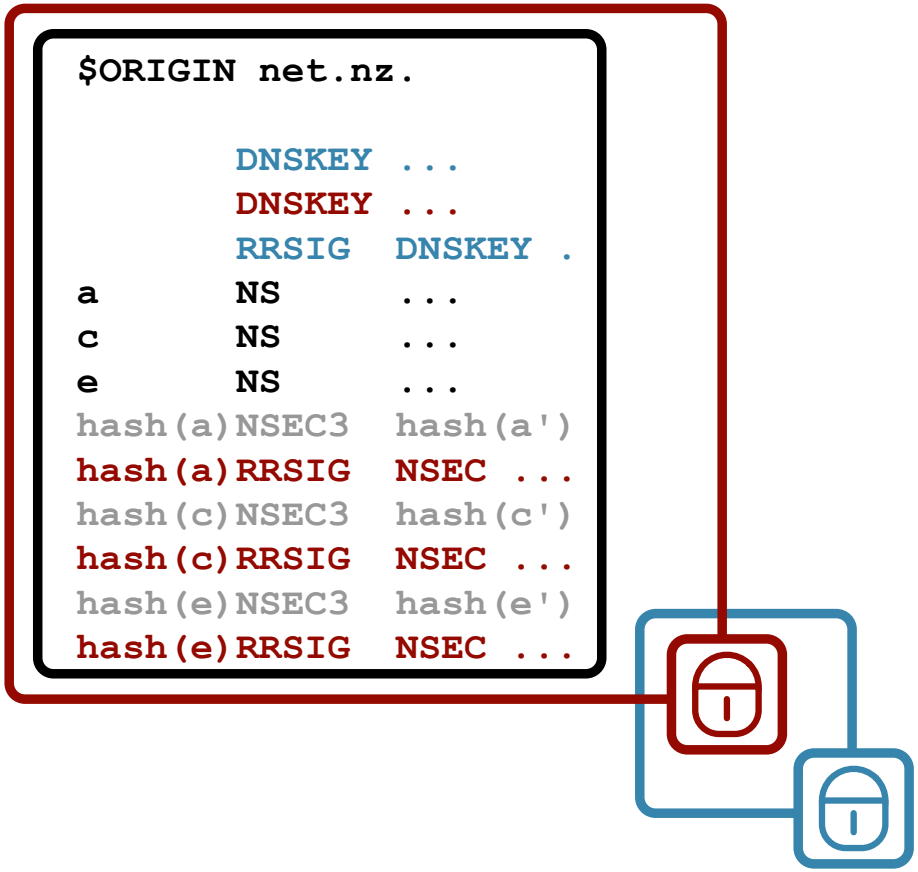


Authentication denial of existence



jay@nzrs.net.nz

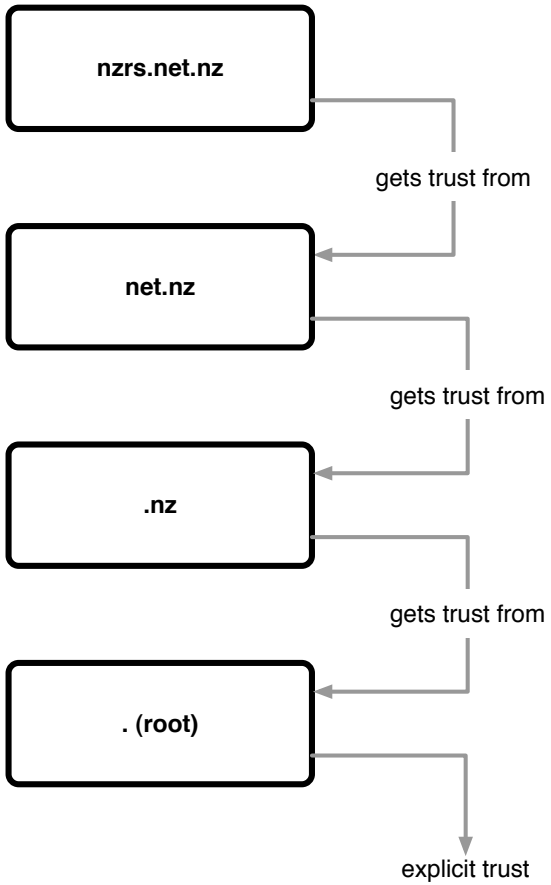
Authenticated denial of existence



Recap

- Purpose
  - Offline pre-generation of answers
  - Don’t allow attacker to control work server does
  - One mechanism prevents enumeration of zone
- Two new Resource Records
  - NSEC : basic chain of empty spaces
  - NSEC3 : chain of empty hash spaces

Chain of trust

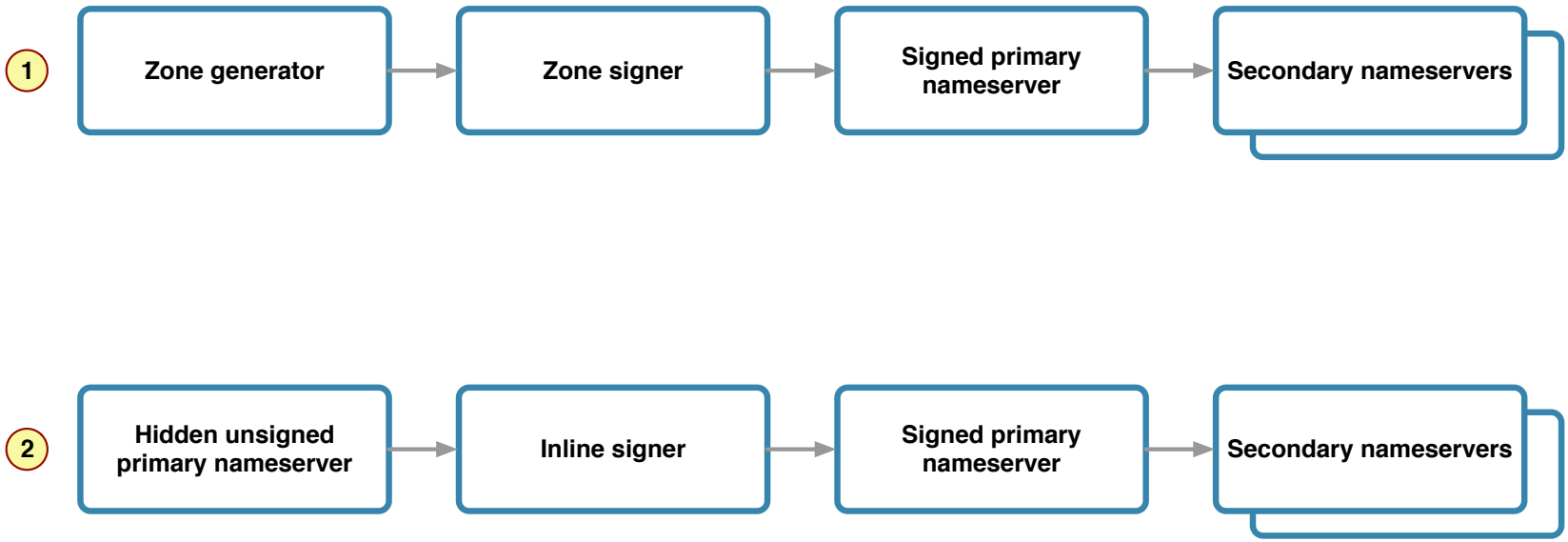


jay@nzrs.net.nz

Operational impact

- New process – signing zones – needs tools
- Key management
- Much bigger zones (up to 12x)
- Timings of
  - Signature lifetimes
  - Key rollovers
  - Backup validity
- Disaster recovery processes

Architecture



jay@nzrs.net.nz

Key management

- HSMs and/or crypto accelerators
  - FIPS what?
  - It can do 2 operations per second, wow!
  - How much?!!
- In case you don't already know:
  - "Every IT department should have a key management policy for all keys."
  - Internal CA

Timings

`http://tools.ietf.org/html/draft-morris-dnsop-dnssec-key-timing-02`

- Initial publication / signing
- Key rollovers
  - Several alternative methods
- Key states
  - generated, published, ready, active, retired, dead, removed
- Signature lifetimes
- Dependencies

Timings

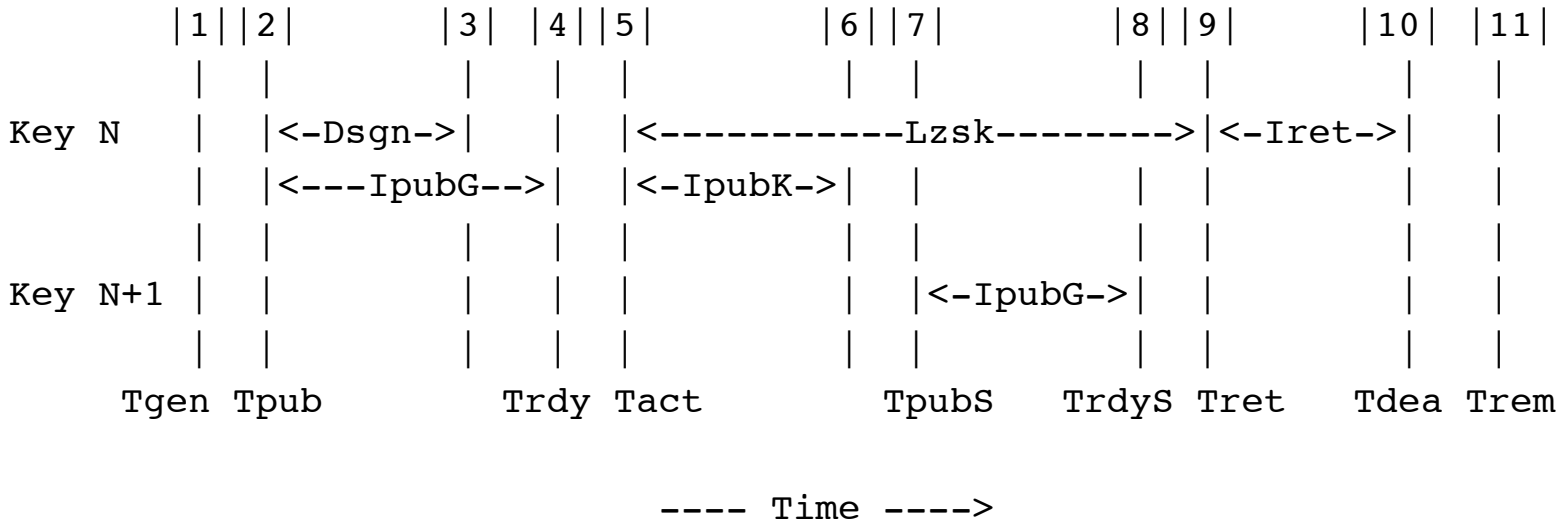


Figure 3: Timeline for a Double-Signature ZSK rollover.

Signing tools – opendnssec.org

- Overview
  - Single piece of software for signing DNS zones that can be seamlessly integrated into an existing system without needing to overhaul the entire existing infrastructure.
  - Can be configured to sign zone files or to sign zones transferred in via AXFR.
  - Fully automatic – once set up, no manual intervention is needed.
  - Possibility of manual key rollover (emergency key rollover).
  - Open source software supplied with a BSD license so suppliers of commercial products can use the open source code in them whilst retaining the IPR of their own software.
- Scalable
  - Able to sign zones containing anything from a few records up to millions of records.
  - Single instance of OpenDNSSEC can be configured to sign one or many zones.
  - Keys can be shared between zones in order to save space in the HSM.
- Flexible
  - Able to define zone signing policy (length of key, key lifetime, signature interval etc.); can set the system up for anything between one policy to cover all zones to one policy per zone.
  - Works with all different versions of the Unix operating system.
- Secure
  - OpenDNSSEC stores sensitive cryptographic data in an HSM, communicating with it using the industry-standard PKCS#11 interface.
  - SoftHSM – a software emulation of an HSM – is available if use of an HSM is not necessary, or to set up a DNSSEC testbed before purchasing a real HSM.
  - Facility to check whether HSMs are compatible with OpenDNSSEC.
  - Includes an auditing function that compares the incoming unsigned zone with the outgoing signed zone, so you can check that no zone data has been lost and that the zone signatures are correct.
  - Supports RSA/SHA1 and SHA2 signatures
  - Denial of existence using NSEC or NSEC3

Timings simplified

- KASP : Key and Signature Policy

```
<Signatures>
    <Resign>PT2H</Resign>
    <Refresh>P3D</Refresh>
    <Validity>
          <Default>P7D</Default>
          <Denial>P7D</Denial>
    </Validity>
    <Jitter>PT12H</Jitter>
    <InceptionOffset>PT300S</InceptionOffset>
 </Signatures>
```

Delegation-only zones

- Remember – NS records are never signed
- New process for accepting DS records
- Decide on whether to use opt-out

DURZ

```
wintermute:~ jay$ dig +dnssec +short @a.root-servers.net . ns

l.root-servers.net.
b.root-servers.net.
h.root-servers.net.
k.root-servers.net.
e.root-servers.net.
m.root-servers.net.
c.root-servers.net.
j.root-servers.net.
a.root-servers.net.
d.root-servers.net.
i.root-servers.net.
f.root-servers.net.
g.root-servers.net.
NS 8 0 518400 20100503000000 20100425230000 55138 .
YhwPaEg3Zss5Ptdf2Vmp5Haa1zfe57PjV2HK1SSzWBntSZrM6wnWmDLU bGAbc
+I5D2vwXXzU+UnLsLQvC64PLU8TiLac1mfYpNW1bsxEbX5gOzl6 5R2HHMkvt9yPaCS/
L2Hu1Bql5JwQY3Ir8lCb6NtMlMWsFwPMFyYqw508 FLE=
```

DURZ keys

```
wintermute:~ jay$ dig +short @a.root-servers.net . DNSKEY

;; Truncated, retrying in TCP mode.
257 3 8 AwEAAawBe++++++++++++++++THIS/IS/AN/INVALID/KEY/AND/SHOU LD/
NOT/BE/USED/CONTACT/ROOTSIGN/AT/ICANN/DOT/ORG/FOR/MOR E/INFORMATION+++
++++++++++++++++++++++++++++++++++ ++++++++++++++++++++++++++++
++++++++++++++++++++++++ ++++++++++++++++++++++++++++++++++++
++++++++++++++ ++++++++++++++++++++++++++++++++++++++++++++++
+ ++++++++++8=
256 3 8 AwEAAavbA++++++++++++++++THIS/IS/AN/INVALID/KEY/AND/SHOU LD/
NOT/BE/USED/CONTACT/ROOTSIGN/AT/ICANN/DOT/ORG/FOR/MOR E/INFORMATION+++
++++++++++++++++++++++++++++++++++ +++++++8
257 3 8 AwEAAazdM++++++++++++++++THIS/IS/AN/INVALID/KEY/AND/SHOU LD/
NOT/BE/USED/CONTACT/ROOTSIGN/AT/ICANN/DOT/ORG/FOR/MOR E/INFORMATION+++
++++++++++++++++++++++++++++++++++ ++++++++++++++++++++++++++++
++++++++++++++++++++++++ ++++++++++++++++++++++++++++++++++++
++++++++++++++ ++++++++++++++++++++++++++++++++++++++++++++++
+ ++++++++++8=
```

DURZ referral

```
wintermute:~ jay$ dig +dnssec @a.root-servers.net nzrs.net.nz a

[Lots omitted]

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;nzrs.net.nz.          IN   A

;; AUTHORITY SECTION:
nz.           172800   IN   NS   ns2.dns.net.nz.
nz.           172800   IN   NS   ns4.dns.net.nz.
nz.           172800   IN   NS   ns7.dns.net.nz.
nz.           172800   IN   NS   ns3.dns.net.nz.
nz.           172800   IN   NS   ns1.dns.net.nz.
nz.           172800   IN   NS   ns5.dns.net.nz.
nz.           172800   IN   NS   ns6.dns.net.nz.
nz.           86400    IN   NSEC om. NS RRSIG NSEC
nz.           86400    IN   RRSIG    NSEC 8 1 86400 20100503000000 20100425230000
55138 . MkMKofMNnEJxu+PS7uNq2myVn9+tQRKGMs2+6nwn3OVidoKThPuAHV5P zUdV/
NczbUiWEx637Cpaafnjm1Fa9ocrnRYsm4QTgGAhS9piOLi9VgsI
0Q32zeKN9ErmDnf6NAZXreN5U2eWZkLM4Cy72/lj+C/pBEIop0kbQT3D 0GQ=
```

Recap

http://www.root-dnssec.org/

- Root now providing DURZ
  - Deliberately Unvalidatable Root Zone
  - Full data size but cannot be used
- EDNS(0) support now vital
  - UDP datagrams larger than 512 bytes
- TCP queries up significantly
- Signed root zone available 1 July 2010 !!

.nz Plans

- Coming later this year
- Need new policies around transfer and so on
- Will use NSEC3 for all zones
- Will use opt-out

Context

- Goal == secure Internet
- Plan == layer by layer
  - Routing : Secure-BGP (on its way)
  - Name resolution : DNSSEC
  - Connectivity : TLS/SSL (er, no, wait)
- But what about before connectivity
  - Up front security?
  - Policies?

Applications in DNS

- SSHFP
  - RFC 4255 : “Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints”
  - New SSHFP resource record for DNS
- DKIM
  - RFC 4871 : “DomainKeys Identified Mail (DKIM) Signatures”
  - Uses _domainkey TXT resource record

Synthesis and redirection

- DNS response depends on the source
  - Load balancing
  - Geo-direction
- Do it properly (anycast) or buy bigger kit

- DNS response depends on the answer
  - Monetisation of NXDOMAINs
- Won't work any more – excellent!

Great Firewall of China

- Computer World: “the incident started just before 10 a.m. [April 8] Eastern Time on Thursday and lasted about 20 minutes. During that time IDC China Telecommunication transmitted bad routing information for between 32,000 and 37,000 networks, redirecting them to IDC China Telecommunication instead of their rightful owners.”

- “These networks included about 8,000 U.S. networks including those operated by Dell, CNN, Starbucks and Apple. More than 8,500 Chinese networks,1,100 in Australia and 230 owned by France Telecom were also affected.”

X.509 confidence trick

- Less than 2 million valid third party certificates
  - But 180 million domains out there !!
- Types
  - Self-signed
  - Domain validation
  - Organisation validation
  - Extended validation
- All vulnerable if root cert compromised

CERT resource record

- Put any key into DNS
- Now we know it came from that domain
- Self-signed – what else do we need?
- Only relies on one root key – the DNSSEC root
- Oh look, it’s a PKI !!

Finish

Jay Daley

Chief Executive, .nz Registry Services

(New Zealand Domain Name Registry Limited)

jay@nzrs.net.nz