DNSSEC Overview

Jay Daley

2009

p: (+64) (4) 931 6977
e: registry@nzrs.net.nz
f: (+64) (4) 931 6979
w: www.nzrs.net.nz
P.O. Box 24361, Wellington, New Zealand
New Zealand Domain Name Registry Limited

DNS is sooo important

- DNS used when you …
  - Visit a web site
  - Send an email
  - Connect to remote file system
  - and more
- Almost every connection you computer makes uses DNS
- Even telephony now uses DNS

Two types of DNS server

- Authoritative servers
  - E.g. those for .nz, .co.nz, .geek.nz
  - Hold the authoritative data
  - Globally distributed
- Caching servers
  - Sort of proxy servers for DNS
  - Hold cached copies of authoritative data
  - Located in Enterprise or ISP

The threat to DNS

- Spoofing of DNS responses
  - You send DNS query
  - Attacker sends forged reply
  - Caching DNS server now misdirected
- Used for
  - Stealing email
  - Pwning web sites (defacement)
  - Redirect customers

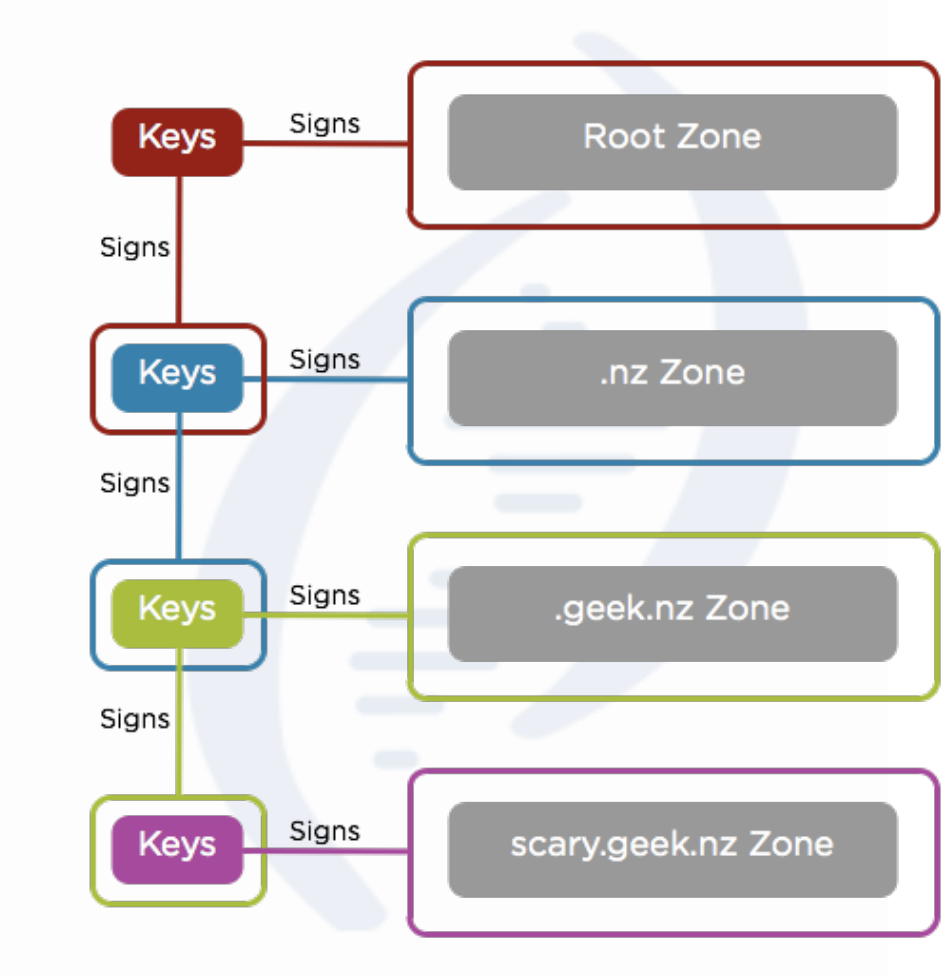
DNS has weak security

- Only check is ID field must match
  - 16 bits = 16,384 packets (not a lot)
- UDP - no source address validation
- Data not checked until cache expiry
- Making exploits:
  - Very difficult to detect
  - Almost impossible to trace
  - Can be attempted all day long

DNSSEC is the solution

- Each zone publishes own keys
  - Keys used to sign DNS responses
  - Each set of keys signed by level above
- Secures authenticity and integrity
- Caching resolvers pass on signatures
  - Or check signatures for you
- Queries are not secured at all

A chain of trust



Layer by layer

- Building a secure Internet
  - Top concern of Internet users
  - Major issue in media and global politics
- DNSSEC is a key building block
  - Each layer secured in turn
  - DNS is fundamental layer
  - Some technologies directly rely on it
    - DKIM -preventing spoofed email

Enterprise impact

- Time to start planning
  - Another reason for a certificate/key management policy and process
  - Aim for end to end security
- Implementation maybe a year away?
  - Still making it into products
  - Root zone not yet signed
- Many things will follow from this

Any questions?

jay@nzrs.net.nz

p: (+64) (4) 931 6977
f: (+64) (4) 931 6979
e: registry@nzrs.net.nz
w: www.nzrs.net.nz
P.O. Box 24361, Wellington, New Zealand
New Zealand Domain Name Registry Limited