



Voco

Application virtualisation

DNS Security

IPv6 - Cryptographically Generated Addresses (CGA)

www.voco.co.nz





Voco

Application virtualisation

www.voco.co.nz

v o c o

Application virtualisation overview

- Applications are packaged
- Contains the application for
 - Security
 - Maintenance of consistent desktop
 - Testing of applications
 - Support for applications with differing requirements
 - Portability
- Provides the ability for IT to be flexible and quick to respond to business needs

How it works

1. Build a “clean” desktop image – preferably a virtual machine
2. Install ThinApp and run – specify the isolation mode
 - a. Merged
 - b. Write Copy
 - c. Full Isolation (requires modification outside wizard)
3. Take a snapshot
4. Install the application(s) - build process
5. Make any configuration changes
6. Start the application for first run
7. Make any configuration/license changes
8. Close the application
9. Take another snapshot
10. Specify executable files that start the virtual application

Some examples

- Skype
- Small scale non standard deployments - for example Visio
- At home use of applications - without requiring a laptop



Voco

DNS Security

www.voco.co.nz



DNS Overview

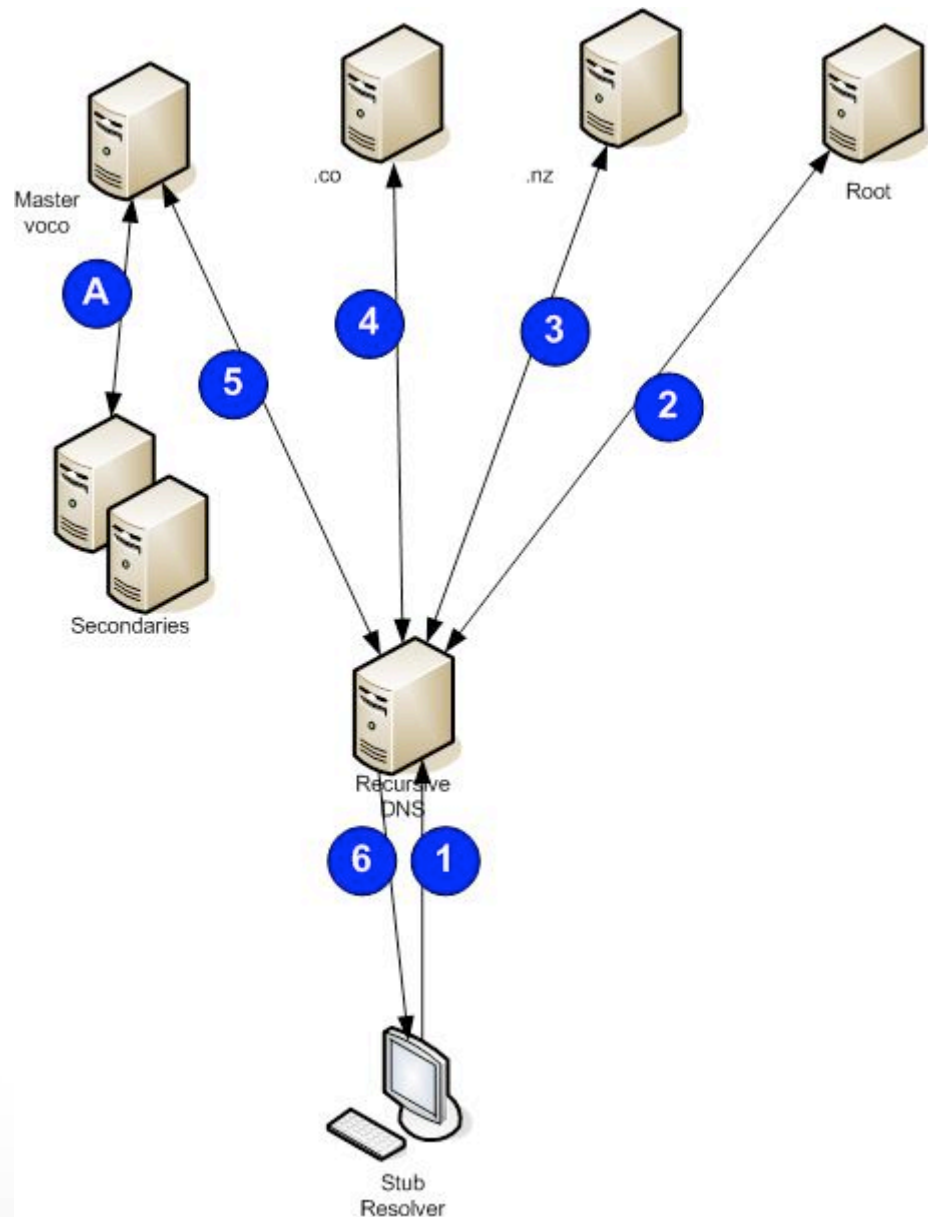
- Provides translation of an easily remembered name to a not so easily remembered IP address (particularly for IPv6!)
 - www.voco.co.nz -> 67.222.96.144
- Is very scalable and simple
 - Small text based exchange of data
 - Low footprint
 - Hierarchical – delegation of authority for easy administration
- Has very simple and weak security
 - Clear text - no encryption
 - Data integrity not provided
 - Transaction id's are used, and until recently were predictable

Without DNS the Internet would not work

DNS Overview

1. Lookup www.voco.co.nz
2. Ask root – try .nz
3. Ask .nz – try .co
4. Ask .co – try voco
5. Ask voco – address resolved
6. Address passed to client

A. Zone transfers



DNS Attacks

- The goal is to send the client to an attackers site instead of the real site typically to:
 - Create botnets
 - Access personal information
 - Damage reputation
- OR deny access to a site

- Typical attacks
 - Unauthorised updates - Dynamic DNS or zone transfers
 - Cache poisoning - client or recursive DNS servers
 - Denial of Service

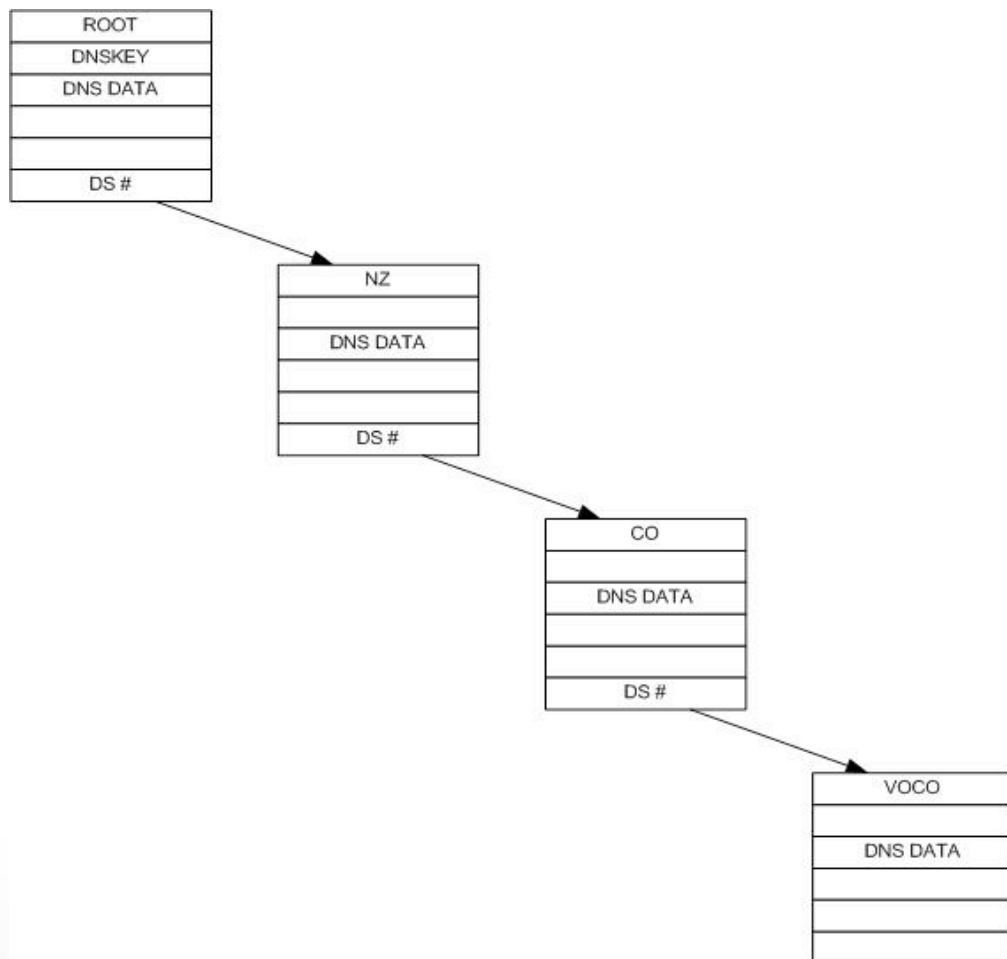
- DNS flaws can overcome other security measures – it is a critical component of life on the Internet

Authentication of communication between Name Servers

- TSIG (2845)
 - Configuration based (i.e. not in zone file)
 - Traffic signed with a shared secret
 - Uses keyed hash authentication codes – low computation hit
- SIG (0) (2931)
 - Uses public key authentication – KEY RR
 - Public key cryptographic operations – high computation hit
- Proprietary
 - Turn off zone transfers
 - Use proprietary mechanisms

Authenticity and integrity of data - DNSSEC

- DNSSEC provides mechanisms to authenticate DNS sources, and therefore significantly increases the security of DNS.
- An Authentication Chain provides trust
- The resource record sets are signed
 - DNS Public Key (DNSKEY)
 - Resource Record Signature (RRSIG)
 - Next Secure (NSEC)
 - Delegation Signer (DS)
- Further reading - <http://www.dnssec.net/>



Considerations

- Client compatibility
 - Secure aware browser must have an anchor
 - Stub resolver will benefit from a security aware recursive resolver
 - Not supported for
 - Windows server 2003 DNS client
 - XP
 - Vista
 - Supported for
 - Windows server 2003 DNS server – but not signing, secondary only, and very early RFC (2535)
 - Windows server 2008 - but not signing, secondary only, and very early RFC (2535)
 - Windows server 2008 R2
 - Windows 7
- Do clients have the correct date
- Standards have changed are still changing

Considerations

- Management overhead
 - More complex
 - Management of keys and signatures
- Root and .NZ not signed until end of this year
- Is there a full secure aware chain
 - Non secure aware DNS devices in the way
 - Load balancing/health checks based on DNS

Key messages

- DNS is critical to the operation of the Internet
- DNSSEC provides security updates that fill in a major gap
- You should investigate if your web site
 - is used for financial transactions
 - represents your reputation
 - provides access to personal information
 - or requires personal information to access
- You could use DNSSEC as a means to distribute public keys for other uses



Voco

IPv6 - Cryptographically Generated Addresses (CGA)

www.voco.co.nz



CGA overview

- Further reading - RFC 3972 and aura-isc2003
- Verifies that the data is coming from the sender address – i.e. anti-spoofing
- Does not verify that the sender is who you think they are
- Does not require a centralised infrastructure

How does it work

- Host address – also called interface id – leftmost 64bits of the 128bit address
- Created from a cryptographic hash of the public key
 - Hash extension techniques can increase the effective hash length beyond 64bits
- The public key is sent to the verifier
- The host address is then verified as the owner of the public key

What is/can it be used for

- IPv6 SEND (secure neighbour discovery)
- Mobile IPv6 binding update authentication
- Opportunistic IPSEC – IETF draft-laganier-ike-ipv6-cga-02
- Positive host identification – DNSSEC + CGA