



# **DNSSEC - Consideration in Selection**

Presented by Lester Kum  
Technical Manager, SGNIC

# Outline

---

- Brief Overview
- How does it work?
- Key Issues/ Concerns
- New Registry Architecture
- DNSSEC Deployment

## Brief Overview

---

- An approach to adding security into the Domain Name System (DNS)
- Why is it needed?
  - Attackers can manipulate DNS responses by inserting fake responses in place of the actual DNS response
  - Attackers can redirect your web browser to point at any address for phishing purposes as an example
  - Man-in-the-middle attacks are hard to detect as such attacks do not change anything on the end-user computers like viruses for example

## How does it work? (1)

---

- A digital signature framework to allow DNS clients to validate the authenticity, integrity and completeness of a DNS response
- Uses the concept of public key cryptography where DNS Resources Records are digitally signed
  - Private key (known only to the DNS zone administrator) is used to sign the zone records
  - Public key (published in the DNS zone) is used to verify the private key that is used to sign the zone records

## How does it work? (2)

---

- Each DNS zone parent is given the role of signing over every delegated child's zone key to verify the child's zone key. This continues until a Trust Anchor (a node in the DNS hierarchy that is always trusted) or the root of the DNS is reached.

## Key Issues/ Concerns (1)

---

- Longer DNS resolution times due to the increased number of DNS transactions required to validate the zone keys
- Increased load on the DNS servers due to the need to re-generate new signatures for all updates performed on resource records in the DNS zone

## Key Issues/ Concerns (2)

---

- Higher client and server data overheads as the average size of a DNS response increases in size significantly due to the additional signature records that are added to the response
  - If the size of the response exceeds the UDP message size, it needs to set the truncated response flag and fall back to using TCP
  - EDNS0 could be used to avoid the expensive overheads of TCP
- More potential points of service failure as trivial zone configuration errors or an expired key can cause serious problems for DNS clients

## Key Issues/ Concerns (3)

---

- The entire contents of a zone file can be reconstructed through the use of the NSEC response in DNSSEC i.e. Zone Walking
  - The solution for zone walking is to use an alternate response to the “No data” situation which would still allow the zone to be signed but would not reveal the entire contents of the zone file as a side effect
  - The NSEC3 approach uses a hash algorithm on the names within the zone so as to increase the cost of zone enumeration to prevent zone walking

## Key Issues/ Concerns (4)

---

- Ability of DNS clients to establish a trusted relationship with all the current DNSSEC signed zones that have no immediate DNSSEC delegation parent
- Ability to use multiple DNS queries which are small in data size to generate many large DNS responses which could serve as amplifiers in Denial-of-Service (DoS) attacks

## Key Issues/ Concerns (5)

---

- Pre-defined behavior of applications required should DNSSEC validation fails
  - Possible to be used as a new form of Denial-of-Service attack to trigger application failure on the end user computer
- Ability to manage the zone keys efficiently. For example, if the private key is compromised, there is no efficient way to revoke the key and inform all child zones quickly

# New Registry Architecture (1)

---

- New registry-registrar system is DNSSEC-ready i.e. Ability to sign the .SG root servers anytime
- The new registry-registrar system utilises DNS Anycast to help facilitate the deployment of DNSSEC
- DNS Anycast
  - A network addressing and routing scheme whereby data is routed to the "nearest" or "best" destination as viewed by the routing topology
  - The new .SG Domain Name System will make use of a primary and secondary DNS Anycast network setup.

## New Registry Architecture (2)

---

- DNS Anycast
  - Beneficial for the deployment of DNSSEC by Improving the performance of the DNS in terms of query response time by distributing the load across multiple geographically dispersed servers

# DNSSEC Deployment

---

- Possibility of conducting a test bed with current secondary authoritative nameserver operators to introduce DNSSEC
  - Might prove to be difficult due to the cost involved in updating the infrastructure versus little customer benefits or cost savings



**THANK YOU!**