DNSSEC Status Report

DNSSEC Public Meeting

ICANN Cairo 2008

SAC 026

- SSAC Statement to ICANN and Community on Deployment of DNSSEC (30 January 2008)
  - Identified DNSSEC deployment issues recommends actions for
    - IANA
    - gTLD and ccTLD registries
    - Registrars
  - Committed to evaluating DNSSEC "readiness" in 7 key areas:
    - Protocol Completeness
    - Key Rollover Process
    - Trust Anchor Repositories
    - Implementation & Deployment Testing
    - Performance and Error Analysis
    - End User Application Development
    - Availability of DNSSEC features on name server platforms

DNSSEC Availability Among Name Servers

- Survey of DNSSEC Capable DNS Implementations (SAC 030)
  - Contacted 40 name server developers and vendors
  - Survey focused on three areas of interest:
    - RFC Support?
    - Interoperability Testing?
    - Key management, encryption support and administrative tools
  - Received vendor assertions from 13 commercial vendors
  - No responses from Open Source developers

Summary

- 65% (11 of 17) products support the core DNSSEC standards today and
  - 3 vendors indicate support by Q1 2009
- 5 products support NSEC3 today
  - 5 anticipate support by Q1 2009
  - 3 others intend to implement but did not identify a timeframe.
- 8 product developers reported that they had done interoperability testing
- 11 products offer some key management applications and DNSSEC-aware utilities.

RFC Support (4033-4035, 5155)

Company (Developer)	Product and Version	Supports DNSSEC RFCs 4033-4035 (Survey Question 1)							Support NSEC3 (RFC5155) (Survey Question 2)		
		Today					Under development	No plans to implement	Today	Under development	No plans to implement
		YES (✓) or NO (✗)	Supports recursion (accept queries with RD=1)	Performs DNSSEC validation	Can act as an authority server	Can host a signed zone and return DNSSEC metadata when requested via DO bit					
Cisco	Cisco Network Registrar and IOS	✗	✓		✓			✗			✗
Infoblox	DNSone	✗					🤔	🤔		🤔	🤔
InfoWeapons	SolidDNS 3.0	✗					Q4 2008			Q4 2008	
INS	Sapphire 3.0	✓	✓	✓	✓	✓				✓	
INS	IPControl 3.0	✓	✓	✓	✓	✓				✓	
ISC	BIND 9.0 (all currently supported versions)	✓	✓	✓	✓	✓				Q4 2008	
Microsoft	Windows Server 2008	✗					🤔			🤔	
Neustar	MetaIP 5.7 Build 6067	✗	✓		✓		Q1 2009			Q1 2009	
Nixu	NameSurfer Suite 6.1.2 (proprietary NS)	✓			✓	✓				Q4 2008	
Nixu	NameSurfer Suite 6.1.2 (Bind 9.3 included)	✓	✓	✓	✓	✓				Q4 2008	
NInet Labs	Name Server Daemon (NSD 3.08)	✓			✓	✓			✓		
NInet Labs	Unbound 1.0	✓	✓	✓					✓		
Nominum	ANS 2.8.2, CNS 3.0.3, Vantio 3.3	✓	✓	✓	✓	✓				✓	
Secure64	Secure64 DNS	✓			✓	✓			✓		
Simple DNS	SimpleDNS Plus 5.0	✗	✓		✓		Jun 2008				✗
Xelerance	DNSX Secure Resolver version 0.9	✓	✓	✓					✓		
Xelerance	DNSX Secure Signer version 1.3	✓			✓				✓		

KEY ✓ Supported ✗ Not supported 🤔 No answer provided

Interoperability Testing

Company (Developer)	Product and Version	YES (✓) or NO (✗)	Interoperability Testing		
			as an authoritative NS to a DNSSEC-aware recursive resolver with these products (Survey Question 4)	as a recursive resolver to DNSSEC-aware stub resolvers with these products (Survey Question 5)	as a DNSSEC-aware stub resolver to a recursive resolver with these products (Survey Question 6)
Cisco	Cisco Network Registrar and IOS	✗			
Infoblox	DNSone	✗			
InfoWeapons	SolidDNS 3.0	✗			
INS	IPControl 3.0	✓	✓	✓	
INS	Sapphire 3.0	✓	✓	✓	
ISC	BIND 9.0 (all currently supported versions)	✓	✓	✓	✓
Microsoft	Windows Server 2008	✗			
Neustar	MetaIP 5.7 Build 6067	✗			
Nixu	NameSurfer Suite 6.1.2 (proprietary NS)	✓	✓		
Nixu	NameSurfer Suite 6.1.2 (Bind 9.3 included)	✗			
NInet Labs	Name Server Daemon (NSD 3.07)	✓	✓		
NInet Labs	Unbound 0.10	✗			✓
Nominum	ANS 2.8.2, CNS 3.0.3, Vantio 3.3	✓	✓		
Secure64	Secure64 DNS	✓	✓		
Simple DNS	SimpleDNS Plus 5.0	✗			
xelerance	DNSX Secure Resolver version 0.9	✗		✓	
Xelerance	DNSX Secure Signer version 1.3	✓	✓		

KEY ✓ Supported ✗ No answer provided

Key Management, Encryption, Administration

Company (Developer)	Product	Product provides key management tools (Survey Question 3)			Encryption Algorithms Supported (Survey Question 7)	DNSSEC-aware Utilities Supported (Survey Question 8)
		Today	Under development	No plans to implement		
Cisco	Cisco Network Registrar and IOS	✗		✗		
Infoblox	DNSone	✗	🤷			
InfoWeapons	SolidDNS 3.0	✗	Q4 2008			
INS	IPControl 3.0	✓			RSASHA1, RSAMD5, DSA, DH, HMACMD5	✓
INS	Sapphire 3.0	✓			RSASHA1, RSAMD5, DSA, DH, HMACMD5	✓
ISC	BIND 9.0 (all currently supported versions)	✓			RSASHA1, RSAMD5, DSA, DH, HMACMD5	✓
Microsoft	Windows Server 2008	✗	🤷			
Neustar	MetaIP 5.7 Build 6067		Q1 2009			
Nixu	NameSurfer Suite 6.1.2 (proprietary NS)	✓	Q3 2008 - Q1 2009		RSASHA1, DSA	✓
Nixu	NameSurfer Suite 6.1.2 (Bind 9.3 included)	✓				
NInet Labs	Name Server Daemon (NSD 3.08)	✓			🤷	🤷
NInet Labs	Unbound 1.0	✓			RSASHA1, RSADSA1, RSASHA256, RSADSA256, RSAMD5	✓
Nominum	ANS 2.8.2, CNS 3.0.3, Vantio 3.3	✓			RSASHA1, RSAMD5, DSASHA1	✓
Secure64	Secure64 DNS		Q3 2008		RSASHA1, DSA	🤷
Simple DNS	SimpleDNS Plus 5.0	✗		✗		
xelerance	DNSX Secure Resolver version 0.9	✓			RSASHA1, RSADSA1, RSASHA256, RSADSA256, RSAMD5	✓
Xelerance	DNSX Secure Signer version 1.3	✓			RSASHA1, DSA	✓

KEY ✓ Supported ✗ Not supported 🤷 No answer provided

Implementation & Deployment Testing

- Tested 24 residential Internet routers and SOHO firewalls
  - Selected devices commonly used with broadband services
- Used controlled test beds to determine whether each unit correctly routes or proxies:
  - DNS queries requiring TCP or EDNS0 to convey lengthy DNSSEC responses
  - Non-DNSSEC queries on signed and unsigned domains
  - Non-DNSSEC queries that set other DNSSEC-related request flags
  - DNSSEC queries that request server-side validation
  - DNSSEC queries that request no server-side validation

Test Findings

- All 24 units could route DNSSEC queries addressed to upstream resolvers without size limitations
- Varying degrees of success with 22 units when proxying DNS queries
  - 6 of 22 DNS proxies had difficulty with DNSSEC-related flags and/or validated responses
  - 16 of 22 DNS proxies passed DNSSEC queries and return validated responses of some size.
  - 18 DNS proxies limited response sizes when DNS runs over UDP
  - Only 4 could process UDP encapsulated responses up to 4096 bytes
  - Majority of units operate in proxy mode when installed using factory defaults
- 25% of units operate are DNSSEC compatibile using default defaults
- 37% of units can be reconfigured to bypass DNS proxy incompatibilities
- 37% of units lack reconfigurable DHCP DNS parameters
  - LAN clients cannot bypass interference with DNSSEC use
- Domain signing will have no impact on broadband consumers that do not use DNSSEC

End User Application Development

- Only informal communication and anecdotal information at this time…
- DNSSEC is not part of standard OS and application builds
- No Windows OS support
  - Vendors and developers cite lack of visibility of DNSSEC through API as major inhibitor
- DNS resolver and validating libraries are available as Open Source or custom builds for Linux, BSD, Solaris, Mac OS X
- DNSSEC validation libraries or patches for
  - Firefox browser and Thunderbird email client
  - Linux and BSD FTP clients (ncftp, lftp)
  - IPSec client (OpenSWAN)
  - OpenSSH

Ongoing Study Items

- Protocol Completeness
- Key Rollover Process
- Trust Anchor Repositories
- Performance and Error Analysis