DNSSEC Deployment Workshop

Steve Crocker
Co-Chair, DNSSEC
Deployment Initiative
November 5, 2008

Cairo, Egypt

Welcome!

- A very full agenda!
- Kaminsky flaw increased visibility
- U.S. Government actions
  - .gov to be signed
  - Notice of inquiry re DNSSEC in root
- Top Level Domains
- Products, Services
- Survey of small routers, firewalls
- DNSSEC recursive resolvers blooming

Signing the Root Discussion

- *The NTIA Notice of Inquiry Regarding*
- *DNSSEC in the Root Zone*
  - Fiona Alexander, Associate Administrator, US Department of Commerce, NTIA
- *VeriSign's Proposal*
  - Pat Kane, VeriSign
- *ICANN's proposal*
  - Rick Lamb, ICANN

DNSSEC In The Field – TLD Registries

- *Bulgaria,* Daniel Kalchev
- *Brazil,* Demi Getschko
- *DNSSEC Launch in .CZ,* Ondrej Filip
- *Public Internet Registry,* Lance Wolak

Routers & Resolvers

DNSSEC Software, Services, Etc

- *Making DNSSEC Accessible to Customers*
  - Uma Murali, Names Beyond
- *DNSSEC in Windows*
  - Shyam Seshadri, Microsoft
- *Appliances & Recursive Resolvers*
  - Steve Crocker

DNSSEC Support in SOHO CPE

"What is the impact of DNSSEC on consumer-class broadband routers"?

- Joint study between Nominet UK and Core Competence
- Conducted July and August 2008
- Expansion of .SE's previous study

Make/Model		DHCP DNS: Out of the Box Usage Mode	No Proxy: Route DNS to Upstream Resolver	UDP Proxy Transport Tests: Proxy DNS over UDP	UDP Proxy DNSSEC Tests: A. EDNS0 Compatibility	UDP Proxy DNSSEC Tests: B. Signed Domain Compatibility	UDP Proxy DNSSEC Tests: E. Request Flag Compatibility	UDP Proxy DNSSEC Tests: D. Checking Disabled Compatibility	UDP Proxy DNSSEC Tests: C. DNSSEC OK Compatibility	TCP Proxy: Proxy DNS over TCP
2Wire	270HG-DHCP	Proxy	OK	OK	FAIL	OK	OK	FAIL	FAIL	FAIL
Actiontec	MI424-WR	Proxy	OK	OK	FAIL > 512	OK	OK	OK	OK	FAIL
Apple	Airport Express	Proxy	OK	OK	FAIL > 512	OK	FAIL	FAIL	FAIL	OK
Belkin	N (F5D8233)	Proxy	OK	OK	FAIL > 1500	OK	OK	OK	OK	FAIL
Belkin	N1 (F5D8631)	Proxy	OK	OK	FAIL > 1500	OK	OK	OK	OK	FAIL
Cisco	c871	Route	OK	OK	FAIL > 512	OK*	OK*	OK*	OK*	FAIL
D-Link	DI-604	Proxy	MIX	OK	FAIL > 1472	OK	OK	OK	OK	FAIL
D-Link	DIR-655	Proxy	OK	OK	OK	OK	OK	OK	OK	FAIL
Draytek	Vigor 2700	Proxy	OK	OK	FAIL > 1464	OK	FAIL	FAIL	OK	FAIL
Juniper	SSG-5	Route	OK	OK	OK	OK	OK	OK	OK	FAIL
Linksys	BEFSR41	Varies	OK	OK	FAIL > 1472	OK	OK	OK	OK	FAIL
Linksys	WAG200G	Varies	OK	OK	OK	OK	OK	OK	OK	FAIL
Linksys	WAG54GS	Varies	OK	OK	OK	OK	OK	OK	OK	FAIL
Linksys	WRT150N	Varies	OK	OK	FAIL > 512	OK	OK	OK	OK	FAIL
Linksys	WRT54G	Varies	OK	OK	FAIL > 512	OK	OK	OK	OK	FAIL
Netgear	DG834G	Proxy	OK	OK	FAIL > 512	OK	FAIL	FAIL	MIX	FAIL
Netopia	3387WG-VGx	Proxy	OK	OK	FAIL > 512	OK	FAIL	FAIL	FAIL	FAIL
SMC	WBR14-G2	Proxy	MIX	OK	FAIL > 512	OK	OK	OK	OK	FAIL
SonicWALL	TZ-150	Route	OK	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Thomson	ST546	Proxy	OK	OK	FAIL > 512	OK	OK	OK	OK	FAIL
WatchGuard	Firebox X5w	Varies	OK	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL
Westell	327W	Proxy	OK	OK	FAIL	OK	OK	FAIL	FAIL	FAIL
ZyXEL	P660H-D1	Proxy	OK	OK	FAIL > 1464	OK	OK	OK	OK	FAIL
ZyXEL	P660RU-T1	Proxy	OK	OK	FAIL > 1464	OK	OK	OK	OK	FAIL

Table 2. Test Result Summary

DHCP Behavior
24 devices tested

A. 3 devices operate only in route mode
B. 6 devices start out in proxy mode and switch to route mode once the WAN link is up up ("chicken and egg" problem)
C. 6 devices start out in proxy mode but can be manually configured to be in route mode
D. 9 devices start out in proxy mode and cannot be configured to be in route mode

All of these will permit clients to route through them if the client overrides the DHCP setting for DNS service

Summary Results

DHCP Behavior	OK Out of the Box	Configurable	Client Routable	Unusable	Total
A. Route	3				3
B. Proxy then Route	2	4			6
C. Proxy; changeable	1	5			6
D. Proxy; not changeable			7	2	9
Total	6	9	7	2	24

DNSSEC Compliant Recursive Resolvers

- End systems typically ask a “recursive resolver”
  - At ISP
  - On premises for large enterprises
- Signed responses only come if asked for
- Therefore, resolvers have to ask

Recursive Resolvers Blooming

- Telia in Sweden operating since 2007
- Comcast in the U.S. just started
- UC Berkeley also operational

- More to come. Data to be collected.

Summary

- DNSSEC is essential
- Sign your zones
- Insist your top level domain be signed
- Insist your partners sign their zones
- Begin checking signatures