DNSSEC Deployment Threats – What's Real? What's FUD?

Steve Crocker, Shinkuro, Inc.
Chair ICANN's Security and Stability Advisory Committee

DNSSEC and IPv6 Workshop 20 Oct 2008

FUD!

- Whoever controls the root key controls the net
- Too complicated
- No business model
- Exacerbates DDoS

Some Real Issues

- RSTEP Report on PIR Application to run DNSSEC
- End user devices
- Chicken-and-egg problems
- Interaction with IPv4/IPv6 translation boxes

RSTEP Report on .ORG DNSSEC

- Thorough look at many possible problems
- Final Recommendation was to go forward

- In tables in the next three slides, the dispositions are
  - A = No action needed
  - B = No a realistic threat
  - C = Normal consideration during pre-op testing
  - D = An area where work is needed

RSTEP Issues with .ORG DNSSEC (1)

Issue	A	B	C	D
Configuration errors will prevent authentication and thus may prevent connections			X	
Lack of a signed root requires other arrangements for distributing the .ORG public key				X
DS records have to be transmitted reliably	X			
PIR is not requiring key change when registrar changes	X			
Fast publication required when the key changes	X			
Need multiple DNSSEC-capable registrars				X
Private key may be disclosed due to improper operation or weakness in the keying algorithm	X			
Signing interval of DS must be consistent with TTL and other timing constraints			X	

RSTEP Issues with .ORG DNSSEC (2)

Threat	A	B	C	D
Need multiple DNSSEC-capable registrars			X	
Registrar may fail to publish keys quickly			X	
Publication of new keys after a rollover may not propagate to all resolvers quickly and reliably			X	
Emergency key rollover is problematic in the absence of a signed root				X
PIR's internal zone signing process may fail	X			
Signing interval of DS must be consistent with TTL and other timing constraints	X			
Registrants may neglect maintenance				X
Private key may be disclosed due to improper operation or weakness in the keying algorithm		X		

RSTEP Issues with .ORG DNSSEC (3)

Threat	A	B	C	D
Zone Signing May be Impractical	X			
Transition Plan for Starting/Stopping DNSSEC		X		
Reporting of DNSSEC Problems				X
Greater Demands Placed on the Servers and Infrastructure			X	
Denial of Service Potential		X		
Getting Validators to Remove the PIR Trust Anchor after the Root is Signed				X

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		Out of the Box Usage Mode	Route DNS to Upstream Resolver	Proxy DNS over UDP	A. EDNS0 Compatibility	B. Signed Domain Compatibility	E. Request Flag Compatibility	D. Checking Disabled Compatibility	C. DNSSEC OK Compatibility	Proxy DNS over TCP
		DHCP DNS	No Proxy	UDP Proxy Transport Tests		UDP Proxy DNSSEC Tests				TCP Proxy
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

	OK Out of the Box	Configurable	Client Routable	Unusable	Total
DHCP Behavior					
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

Chicken-and-Egg Problems

- Signing versus Validating
  - No need to check signatures until enough zones are signed
  - No need to sign zones until enough validators are checking signatures
- Top down, bottom up, inside out?
  - Wait for the root to be signed and then the TLDs
  - Work from the bottom and apply pressure upward
  - Sign early adopters and work up, down and sideways
- Need a Trust Anchor Repository…

Trust Anchor Repository

- Need a way to distribute keys of signed zones with unsigned parents
- Resistance because it's…
  - An additional structure, more work
  - Not standardized
  - Another trust model
  - Might last too long

- On the other hand, it completely solves the problem of initial operation

Registrars

- Need registrar support to connect enterprises to registries
- Many small businesses do not run their own DNS
  - Registrar runs it for them
- We need to get at least a few registrars up able to run DNSSEC
  - We are supporting NamesBeyond. Willing to work with others.

IPv4/IPv6 translation

- Growing attention on co-existence of IPv4 and IPv6 networks
- Various forms of Network Address Translation boxes now being promulgated
- Some strategies involve rewriting answers to DNS queries
- Not clear how to integrate with DNSSEC

- Personal Opinion: IPv4/IPv6 translation is an overlay network. Overlay network requires a separate trust model. DNSSEC is part of, but the complete answer.