DNSSEC History, Status, Future

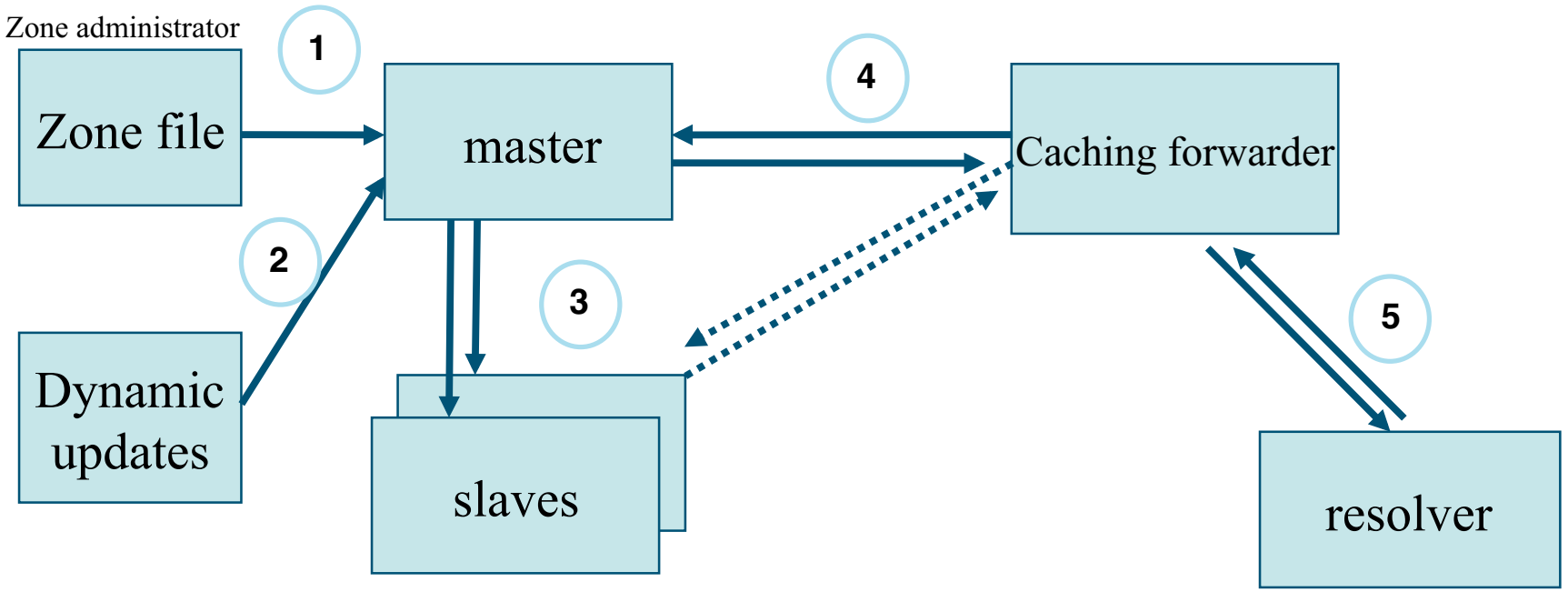
Steve Crocker, steve@shinkuro.com, Shinkuro, Inc.
Chair ICANN's Security and Stability Advisory Committee

Internet Dagarna 21 Oct 2008

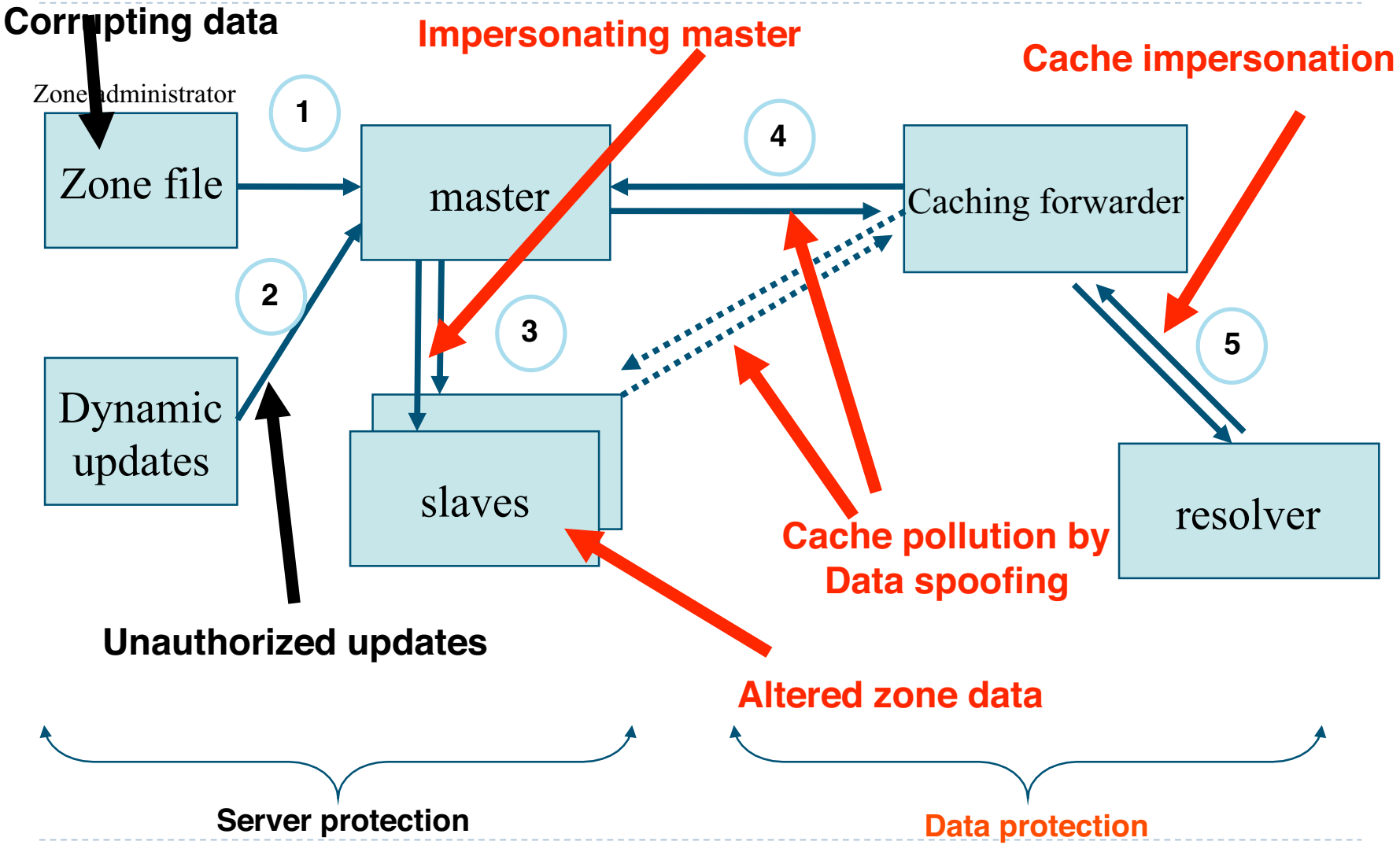
Outline

- Introduction and history of DNSSEC
- Current status of implementation and deployment
- Experiences from early adopters
- Obstacles that hinder the roll out of DNSSEC
- The future development of DNSSEC

DNS: Data Flow



DNS Vulnerabilities



How bad can it get?

- In wireless environments, it's easy to substitute DNS responses.
- Redirect to a false site
  - Steal passwords
- Redirect to a man-in-the-middle site
  - See and copy an entire session
  - Web, email, IM, etc.
- **And, of course, Kaminsky's attack**

Where Does DNSSEC Come In?

- DNSSEC secures the name to address mapping
  - Transport and Application security are just other layers.

DNSSEC hypersummary

- Data authenticity and integrity by signing the Resource Records Sets with private key
- Public DNSKEYs used to verify the RRSIGs
- Children sign their zones with their private key
  - Authenticity of that key established by signature by the parent

History – Design Process

- Demonstration of Cache Poisoning in early 1990s
  - Raised concern at high levels in the U.S. Government
  - Caused initiation of DNSSEC design work
- Three major design iterations for more than a decade
  - Basic design is straightforward
  - Distributed key management didn't scale well in early designs
- "Final" design standardized in RFC 4033-35 March 2005
- Additional privacy requirement emerged
  - NSEC3 standardized March 2008, RFC 5155
- Key Rollover Scheme using Timers
  - RFC 5011, September 2007

The Deployment Process

- Deployment is separate from design and standardization
- Software products, tools
- Documentation – tutorials, manuals, etc.
- Services
- Early adopters
  - Zone signers
  - Validators

- Loose ends…

Top Level Domain Leaders

- Sweden
  - .SE first implementation of a top level domain
  - Formal launch of commercial DNSSEC service February 2007
  - .MUSEUM now signed too
- Bulgaria, Puerto Rico, Brazil, Czech Republic
- Coming soon: .ORG, India, United Kingdom, Mexico, U.S. Government, …
- Coming a bit later: root, COM, NET

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

August 22, 2008

M-08-23

MEMORANDUM FOR CHIEF INFORMATION OFFICERS

FROM: Karen Evans
Administrator, Office of E-Government and Information Technology

SUBJECT: Securing the Federal Government's Domain Name System Infrastructure
(Submission of Draft Agency Plans Due by September 5, 2008)

The efficient and effective use of our networks is important to promote a more citizen centered

New Policy

This memorandum addresses two important issues in following through with the existing policy and expanding its scope to address all USG information systems.

A. The Federal Government will deploy DNSSEC to the top level .gov domain by January 2009. The top level .gov domain includes the registrar, registry, and DNS server operations. This policy requires that the top level .gov domain will be DNSSEC signed and processes to enable secure delegated sub-domains will be developed. Signing the top level .gov domain is a critical procedure necessary for broad deployment of DNSSEC, increases the utility of DNSSEC, and simplifies lower level deployment by agencies

Validation in Recursive Resolvers

- Telia – Large ISP in Sweden
- Comcast – U.S. ISP
- University of California, Berkeley
- (India)

Software Leaders

- Internet Systems Consortium (ISC) – Bind
- NLnet Labs – NSD
- Sparta – various tools
- Several others

Problem Areas

- Seamless adoption for domain holders
- Seamless adoption for users

- End system compatibility
- Trust Anchor Repository
  - Root Signature
- Registrar support
- Productized software
  - All the rough edges smoothed out
- IPv4/IPv6 translation gateways

DNSSEC Support in SOHO CPE

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

- Accidental discovery of problem last year in Swede
  - (Gavle disappeared)
- .SE study of problem
- Joint study between Nominet UK and Core Competence
- Conducted July and August 2008
- Expansion of .SE's previous study

Make/Model		DHCP DNS	No Proxy	UDP Proxy Transport Tests		UDP Proxy DNSSEC Tests				TCP Proxy
		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
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

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.

Root Activities

- IANA's Interim Trust Anchor Repository (ITAR)
  - Web-based publication of keys for signed TLDs
  - Temporary measure until the root is signed
- U.S. Dept of Commerce NTIA Notice of Inquiry
  - www.ntia.doc.gov/DNS/dnssec.html
- ICANN's DNSSEC Implementation
  - Hardware-based implementation of DNSSEC for root, .ARPA, etc.
  - www.ntia.doc.gov/DNS/ICANNDNSSECProposal.pdf
- VeriSign's DNSSEC Implementation
  - Test bed for signing the root
  - www.ntia.doc.gov/DNS/VeriSignDNSSECProposal.pdf

DNSSEC Future

- The Root will likely be signed (6 to 24 months)
- More major ccTLDs and gTLDs will be signed
- Announcements by major software vendors
- Deployment in registrars
- Incorporation in end systems

Summary

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

Resources

- www.dnssec-deployment.org
  - Includes monthly newsletter, DNSSEC This Month
- DNSSEC Deployment Mailing list
  - dnssec-deployment-subscribe@shinkuro.com
- www.dnssec-tools.org/
- www.dnssec.net/
- www.isc.org
  - Internet Systems Consortium – BIND, DLV
- www.nlnetlabs.nl
  - NLnet Labs – NSD, Unbound