# DNSSEC Goes Mainstream: Deployment Incentives, Experience, and Questions

Suzanne Woolf, ISC

# Introduction

- What's DNSSEC and what problem does it solve?
- OK, so why isn't it deployed yet?
  - Economics
  - Operations
- What do you mean, it's being deployed?
- So what do I do now?
  - Experience we've had
  - Experience you can be part of

# What's DNSSEC?

- Adds authentication to the DNS
  - Digital signatures (public key crypto)
  - Carried in DNS resource records
  - You know the message you got is what was sent
- That's all. Really.
- Does not:
  - Hide or encrypt anything
  - Prevent DDoS or otherwise protect servers

# What Problem does DNSSEC Solve?

- Vanilla DNS is credulous enough to believe almost anything from almost anybody
- Once it’s believed a bad answer, a resolver will keep repeating it, too.
- Some basic street smarts added over the years, but DNS is still pretty naive

# Is This a Problem We Actually Have?

- Attacking DNS was simple, but attacking other things was even simpler
  - People (phishing)
  - Machines (worms/viruses)
  - Networks (compromised routers, hijacked addresses)
- So, for a long time: Nope, it’s not.

# All Dressed Up, No Place to Go

- DNSSEC standards issued in 2004.
- Support in widely used open source nameservers also in 2004
- And we waited
  - Costs some, in resources (bw, cpu, clue)
  - Benefits unclear (the usual chicken-and-egg, and didn’t solve a really pressing problem)

# So Why Are We Here?

- Remember about cache poisoning? Not a problem we have, right?
- March 2008, Dan Kaminsky discovers a way to turbocharge a well-known attack.
- Now cache poisoning is a problem we have.
- Remember DNSSEC? Awkward, expensive, not clearly good for much?
- Now DNSSEC solves a problem we have.

# Overnight Success

- A handful of TLDs are signed now
  - .se signed last year
  - .gov signed early this year
  - .org signed in the last couple of weeks
- Other TLD operators are evaluating
  - Informally discussed plans for .mil, .edu, .uk, others....maybe even .com?
- IANA is publishing TLD trust anchors
  - Root is not signed
  - But there's a list of trust anchors from IANA

# Oh and the root zone....

- Authority here is US Department of Commerce
  - Notice of Inquiry on DNSSEC, Oct. 2008
  - Key management gets wrapped in Layer 9
- Announced cooperative effort with ICANN and Verisign on “an initiative to enhance the security and stability of the Internet.”
  - Interim plan, recognizes experience and evolution are needed
  - Goal is year-end deployment

# Root zone mechanics

- ICANN's role
  - Operates IANA, due diligence on all root zone changes
- Verisign's role
  - Generates the root zone
  - Manages zone signing keys
- NTIA's role
  - Continue to audit changes to root zone
  - Final decisions on management of key signing keys (joint plan of Verisign and ICANN)

# Early experience: .gov

- .gov live in Feb 2009
  - Formally announced Sept. 2008
  - Goal is for subdomains to be signed Dec. 2009
- Signed with NSEC3
  - NSEC3 prevents enumeration of zone
  - Newer variant, some unknowns
- Early results are encouraging
  - Registry interface works
  - Key rollover events successfully performed
  - .gov key in IANA TLD key repository

# Things to ponder: EDNS0

- EDNS0 extension to DNS “modernizes” the protocol
  - Packet size negotiation
  - Option fields
- EDNS0 with DO option set is required for DNSSEC
  - “DO=1” = “I won't die if I see DNSSEC data”
  - Assumes large enough packets to carry larger answers
  - Often set by default

# Things to ponder: packet sizes

- EDNS0 provides for packet size negotiation
  - Starts large
  - Falls back smaller and smaller
  - Can go down to 512 bytes
- What if DNSSEC answer doesn't fit in negotiated packet?
  - TC bit (truncate) is set
  - Triggers fallback to TCP, which doesn't scale
  - Protocol fix under discussion: ignore DO if packet size is inadequate

# Things to ponder: middleboxes

- Many stateful firewalls think they know what DNS packets look like
- DNSSEC-Signed answers are different
  - DNSSEC RRs do not look like other RRs
  - EDNS0 packets do not look like older DNS packets
- Much SOHO gear does the wrong thing by default, which can result in dropped answers.

# Things We Still Don’t Know (1)

- Uptake further down the tree
  - Business case for DNSSEC: what risks does it really mitigate?
  - Does having DNSSEC change anything if you don’t use it?
  - How much is the resource commit, really?
- Widespread DNSSEC: what changes?
  - Scaling DNS (including the root zone)
  - Expectations: does a more trustworthy DNS enable other things?

# Things We Still Don't Know (2)

- Key management is important.
  - Rollback is hard
  - Still evolving BCPs on algorithms, lifetimes, and other key characteristics
  - Where do you put them? (a TARpit)
- It’s still hard to get people to pay for security
  - Registrars see no value proposition
  - TLDs are not charging

# Conclusions

- DNSSEC is fairly complex technology
- That solves a problem we have, now
- With some costs,
- Providing some new potential, so
- *If you've been waiting for DNSSEC to be "for real", your time is now.*
  - If you manage DNS zones, look into signing them
  - If you run large resolvers, look at what will happen when you're receiving signed data

# And a little help from our friends

- Folks here from:
  - Comcast DNS group
  - Afilias (.org operator)
- DNSSEC Signed Root Deployment Symposium
  - Gathering of DNSSEC experts June 11-12
  - Results appearing soon
- Ongoing data-gathering by early adopters