

# Securing the DNS

## An ISOC Briefing Panel

Leslie Daigle

July 28 2009, Stockholm

# Welcome!

- We're very pleased with the interest in this session
  - we are being live audiocast
  - audiocast & transcript will be available for later download
- This is not a “technical debate”
  - IETF is next door
  - we're pulling the message out of engineering and talking to the “real world”

# Today's Topic: the Domain Name System

- The DNS...
  - core infrastructure for Internet applications
  - global, yet highly distributed
    - data updates are done “close to the source”
  - effective and efficient
  - has scaled

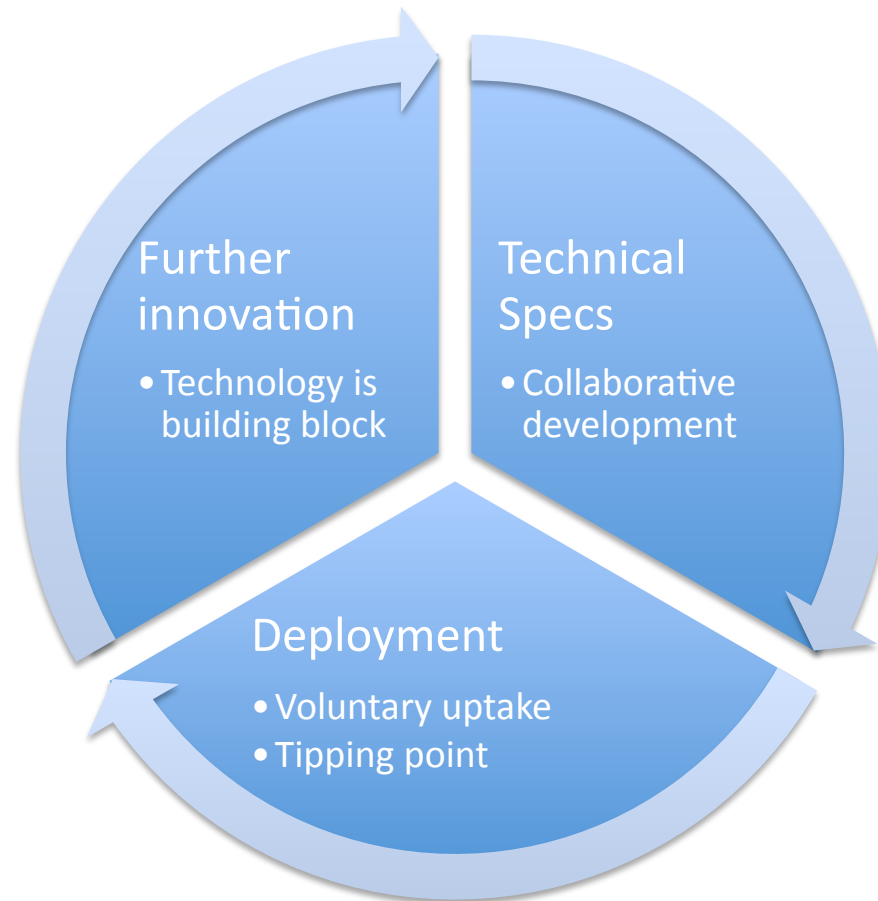
# Securing the DNS

- “Threats” to the DNS, as any infrastructure, come in many flavours
  - configuration errors
  - connectivity issues
    - including DOS
  - conflicting operational practices
- Solutions are also varied
  - better software
  - adoption of “best practices”
  - dealing with DOS
  - allowing authentication of DNS responses

# DNSSEC

- Enables: verification that a DNS response is as the zone administrator intended
- Uses public key cryptography
- Requires general uptake throughout the DNS hierarchical infrastructure
  - At least top to bottom
- Does not address all threats (previous slide)
- Does provide building block for supporting more security in all applications and services

# Standards->Deployment Cycle



We are here!

# So...

- DNSSEC is not an academic exercise
- Panel: experts and key infrastructure operators
- Discussion: current status and opportunities looking forward

# The Panel

- Olaf Kolkman
  - IETF development of DNSSEC and technical development experiences
- Patrik Wallström
  - DNSSEC the .SE way - why, when, what
- Jim Galvin
  - Experiences and opportunities encountered in driving adoption of DNSSEC across registries and registrars
- Matt Larson
  - DNSSEC on .com, .net and the root
- Richard Lamb
  - DNSSEC at the root - opening the door to opportunity?