DNSSEC Deployment

Bill Manning channeling a presentation of Steve Crocker
Shinkuro, Inc.
plus some additional data from Verisign
August 31, 2004



What is DNSSEC?

- Cryptographic signatures in DNS
- Assures integrity of DNS query results
 - Protects against tampering in caches, transmission
- End-system checks signature chain up to root
- Key Internet infrastructure strengthening step
 - Routing & DDoS suppression are the other key steps



History & Status

- DNS threats identified in early 1990s
- DNS Security Protocol design started
- >10 years to complete the specification(!)
 - Three major iterations, each with prototype implementation and testing
- Specification emerging now from the IETF



The Deployment Process

- Specification and Design
- Implementation
- Testing
- Productization

- Education/Marketing
- Adoption
- Training
- Operation
- Incident Handling

- ✓ Mostly done
- o In process
- To be started

Lots of Work

Still to be Done



Broad "Epochs"

- Empty The current status
- Isolated Just a few zones are signed
- Sparse A large number but a small fraction
- Dense A large fraction
- Complete Someday...

Challenge: Manage the Isolated and Sparse periods; spur adoption



ICANN Roles

- IANA is pivotal point for Root
 - Signing the root requires IANA, DoC, and Root Servers cooperation and new procedures
- SSAC
 - SSAC has examined deployment issues
 - Level of effort exceeds SSAC capability
 - New project created



The DNSSEC Deployment Project

- Structure ("Virtual Program Management")
- Government Funding
- Major Players and Objectives



- Build and Refine Road Map
- Measure Progress
- Identify Issues
- Organize solutions

Open and Inclusive Process

The DNSSEC Road Map

- Major operating components
 - End-systems
 - Nearest DNS resolver
 - Recursive resolvers
 - Caches and Secondaries
 - Authoritative zone servers
 - Registries (TLDs) and Root
 - Registrars

Issues - 1

- Root Key
 - How to distribute
 - Who controls it
 - How to roll it over
- End Systems
 - What do end systems do while DNSSEC is only sparsely available

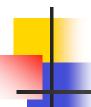


Trust Anchors

- Multiple "Secure Entry Points" during early epochs
- How to distribute keys and inform end systems

Privacy

 DNSSEC enables "zone walking" to learn the full set of names in a zone



Funding and Management

- U.S. Dept of Homeland Security
 - Other government funding desired...
- U.S. Leadership
 - Russ Mundy, Steve Crocker, NIST
- European Leadership
 - Johan Ihren, Olaf Kolkman, et al.
- Asia-Pacific Leadership
 - Jun Murai, et al.
- Steering groups being formed



Major Groups & Objectives

- IANA, Root Server Operators
- gTLDS
- ccTLDs
- DNS software vendors
- Major organizations
- ...



A TLD specific issue



DNSSEC Provisioning

- Registrant generates a public/private key pair for a zone
- Registrant signs the zone with the private key
- Registrant sends the zone's public key to the registrar
- Registrar sends registrant'skey to the registry
- Registry puts registrant'skey hash (DS) in the TLD zone
- Registrysigns the TLD zone
- Registry publishes signed TLD zone