Wild Card Report
(Redirection in the COM and NET Domains)

Steve Crocker
SSAC Chair
July 21, 2004

www.icann.org/committees/security/ssac-report 09jul04.pdf

SSAC: Security and Stability Advisory Committee

- An advisory committee to the ICANN board
- Volunteers – individual, technically competent, unpaid
- SSAC operates semi-independently
  - Does not speak for ICANN
  - Focuses on security and stability, not politics or contracts

Background

- 15 Sept 2003 – VeriSign changed COM and NET domain registries
- Queries of uninstantiated names – usually typographical mistakes – were redirected to VeriSign's servers instead of receiving the standard error code.
- Community response was swift and vocal
- VeriSign suspended the change
- SSAC held meetings in October

Findings 1-4

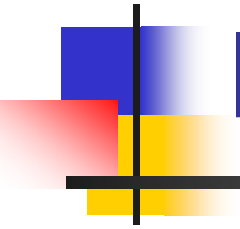
1. VeriSign changed the registry; caused harm
2. The Change violated engineering principles, blurred architectural layers
3. VeriSign's Change put itself in the loop for all current and future protocol changes
4. The Change was abrupt despite long internal development

Findings 5-8

5. Quick reactions yielded more changes and counterpatches
6. Email senders and receivers were ingested into VeriSign servers
7. Web redirection program collected information associated with users
8. The collective events reduced trust overall

Recommendations

1. No new wild cards in TLDs
2. Roll back wild cards in existing TLDs
3. Clean up specs
4. Enforce proper discipline, including open notice and consensus, for registry changes

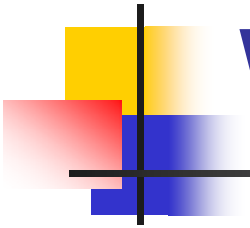


DNSSEC Deployment

Steve Crocker

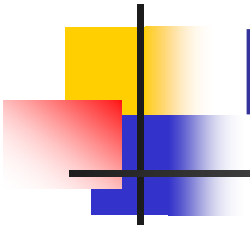
Shinkuro, Inc.

July 21, 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
- o Implementation
- o 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

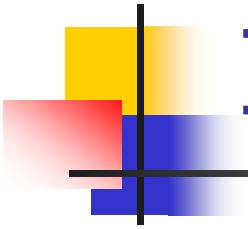
“Virtual Program Management”

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

- Open and Inclusive Process

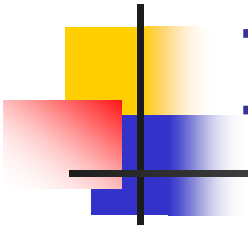
The DNSSEC Road Map

- 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



Issues - 2

- 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.
- Steering groups being formed

Major Groups & Objectives

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