Security and Stability Advisory Committee

Steve Crocker, Chair
July 22, 2004
Kuala Lumpur, Malaysia

steve@stevecrocker.com

SSAC Committee

- **Steve Crocker, Chair**
- **Alain Patrick Aina**
- **Jaap Akkerhuis**
- **Steven M. Bellovin**
- **Rob Blokzijl**
- **David R. Conrad**
- **Johan Ihren**
- **Mark Kosters**
- **Allison Mankin**
- **Ram Mohan**
- **Russ Mundy**
- **Jun Murai**
- **Frederico A.C. Neves**
- **Ray Plzak**
- **Doron Shikmoni**
- **Ken Silva**
- **Bruce Tonkin**
- **Paul Vixie**
- **Rick Wesson**

Staff support: Jim Galvin

Rotation and Replenishment

- SSAC formed in spring 2002
- Initial members selected by ICANN staff
- Very few changes since then
  - Two additions and two departures
    - One departure was pro forma
- Now looking for new members
- Interview process underway

SSAC Fellow

- Jim Galvin has been part time exec dir
- Need full time researcher and writer
- Announcement posted
  - Evaluation in progress
  - May not result in selection

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

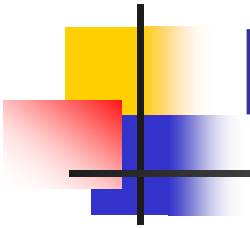
www.icann.org/committees/security/ssac-report 09jul04.pdf

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

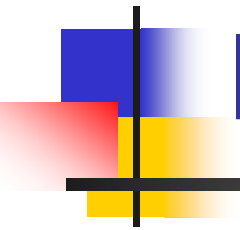


Findings 5-8

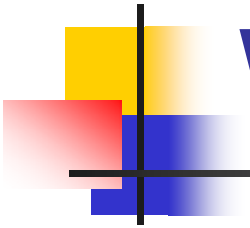
5. Quick reactions yielded more changes and counterpatches
6. Email senders and receivers were ingested into VeriSign servers
7. Web redirection page collected information associated with users
8. The collective events reduced trust overall

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

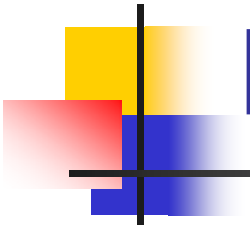


DNSSEC Deployment



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…

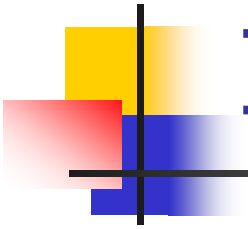
Challenge: Manage the Isolated and Sparse periods; spur adoption

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

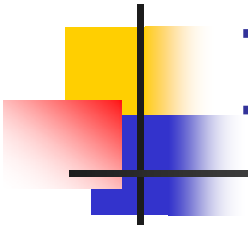
The DNSSEC Road Map

- 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