Security and Stability Advisory Committee – Current Activity

Steve Crocker Chair
Security and Stability Advisory Committee
March 5, 2004
Rome, Italy

steve@stevecrocker.com
New Acronym

- Was SECSAC
- Now SSAC – “ess sac”
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
SSAC Committee Strengths

- Root Server Operators
- gTLD Operators
- ccTLD Operators
- Name Space Registries
- Regional Internet Registries (RIRs)
- Registrars
- Internet Security

No policy or political members(!)
Selected Current Topics

- Wild Card
- New TLDs
- DNSSEC
- Rotation and Replenishment
Wild Card

- VeriSign used the wild card feature in DNS to redirect queries to uninstantiated domains
- Lots of community pushback
- SSAC held meetings on Oct 7 & 15
- Report is overdue. Committee will have draft by end of March
- Further complicated by lawsuit
New TLDs

- Pressure on the root?  Not much
- Pressure on the IANA?  Yes
- Business continuity?  Will fail
DNSSEC

- DNSSEC is signature protocol for DNS entries
- Each entry signed; traceable back to root
- Provides strong assurance of authenticity of response
- Doesn’t solve all security issues, but tightens one important element of the overall system
DNSSEC Status

- DNSSEC has been brewing for a long time
  - 10 years(!), 3 major iterations of the specs
- Specs are just now being finalized
- Some trials and interoperability experiments
- No actual deployments yet
DNSSEC Roll Out

- Specs
- Design
- Implementation
- Products
- Education (Marketing)
- Deployment
- Training
- Operation
Problems, Policies

- Root Key
  - Control and management
  - Rollover
  - Distribution
- Operation during sparse deployment
- End system behavior when/while signatures do not exist
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
- Need process for replacing members
  - Needs to be fair, balanced but not mindless
  - Focus will continue on competence, independence of view
- No natural constituencies
- Will structure a process and put it into operation
  - Will try to move this forward by KL
  - Suggestions for process and specific candidates are welcome