ICANN Security and Stability Advisory Committee

ICANN Meetings

Shanghai

October 30, 2002

Committee

- **Steve Crocker, Chair**
- **Alain Aina**
- **Jaap Akkerhuis**
- **Doug Barton**
- **Steven M. Bellovin**
- **Rob Blokzijl**
- **David R. Conrad**
- **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**
- **Stuart Lynn, ex-officio**

Staff support: Jim Galvin

Committee Strengths

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

No policy or political members(!)

Topics

- General progress
- Zone transfer
- Root and TLD denial of service attack
- Whois Accuracy

Strength

- **Protocols:** The protocols are well defined and well designed
- **System Design:** The system of servers and communication paths is strong and robust against both qualitative attacks, e.g. source address spoofing, and quantitative attacks, e.g. DDOS.
- **Registration:** The registration procedures are strong and reasonably uniform
- **Threats:** The threats are identified and countered

Measurement

- Metrics and Milestones
  - What constitutes “good?”
  - Partly quantitative and partly qualitative
- Measurements
  - Where are we?
  - How quickly are we improving?

Make sure we’re all talking about the same things – avoid vague hyperbole

Long term schedule

- Plot course toward acceptable state
  - Probably a couple of years
- Shift into maintenance mode
  - Re-evaluate charter, organization, operation

Near term schedule

- By Shanghai…
  - Description
  - Vulnerabilities
  - Security Architecture
  - Measurement framework

Actual Progress

- Framework is coming along
- Details progress is slower than desired
- Will shift to individual recommendations on a quicker schedule
- “Current events”

The Distributed Denial of Service (DDoS) Attacks

- Attack was substantial and serious, but…
- Damage to end users was minimal
  - Concurring with RSSAC, et al..
- Structure is sound – good redundancy and diversity
- Operators responded well
- Some servers suffered under the load
  - But none broke
- Capacity and rapid response from operators was the key.

DDoS -- Improvements

- Direct improvements in DNS
  - Strengthen the servers and operations
- Generic improvements against DDoS
  - Secure the edge
  - Reduce number of easily captured (porous) hosts

SAC actions

- Work with RSSAC, et al on a report
- Extend SAC activity to include operational issues
- Open a dialog on the generic DDoS security issue

Zone Transfer Controversy

- ICANN/IANA asked SAC to comment on procedures involved in zone transfer
- Extended controversy; SAC focus is on security

SAC comments on AXFR

- Essential requirements
  - Authentication of request(or)
  - Consistency between parent and child
- Desirable requirements
  - Good glue; accurate IP addresses of the nameservers.
  - Clean data, e.g. well-formed host names of nameservers
  - Up to date version of BIND or other software
  - Redundant, reliable servers, preferably geographically distributed
  - Disaster recovery preparations

SAC actions on AXFR

- ccTLDs, IANA and SAC have formed small, short term working group to resolve procedures

SAC comments on gTLD Whois

- To ICANN
  - Last verified date
  - Privacy is needed
  - Standard format be developed
- To IANA
  - Publicly available list of WHOIS servers