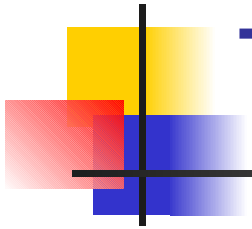
Security and Stability Advisory Committee

Public Forum Presentation

Mar del Plata

April 6, 2005

Steve Crocker, chair
steve@stevecrocker.com

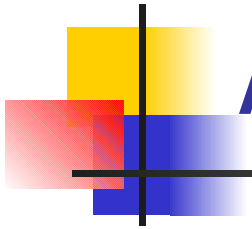


Topics

- Structure
- Activities
- DNSSEC
- Domain Name Hijacking

Structure

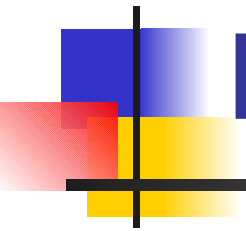
- Committee of roughly 20 experts
  - All volunteers
  - All technical
  - Broad participation across component constituencies
- Board committee
  - Advised both the board and the overall community



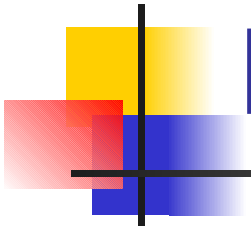
Activities

- DNSSEC
- Domain Name Hijacking

- Add Storm
- Phishing
- etc

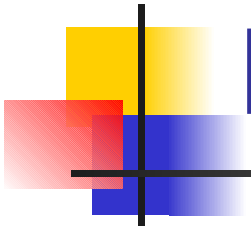


DNS Security



DNSSEC is…

- … “DNS Security” Protocol
- … protection against tampering
  - domain name and address are tied together
- … an extension to the DNS protocol
- … a twelve year technical development
- … finally published by the IETF
  - RFCs 4033, 4034, 4035
- … ready for deployment



DNSSEC Deployment is…

- … the transition from specs to operation
- … a multinational effort
- … a complex process
- … a project that needs your help

ICANN and DNSSEC

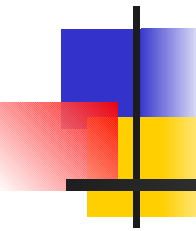
- ICANN
  - IANA signs the root
  - Coordination with the TLDs
  - Community Leadership
- Many other participants
  - Governments
  - ISPs, DNS operators
  - Enterprises
  - Software Vendors

What's Happening Now?

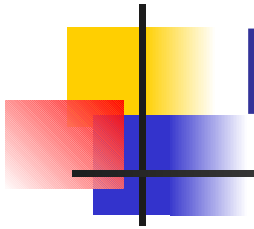
- Roadmap Development
- Workshops and Test Beds
- Software Development
- Early adopters
- Preparation for signing and deploying root
- Top level domains
- Selected applications

What's the Schedule?

- 2005
  - ✓ Specs published (RFCs 4033, 4034, 4035)
  - ✓ Road map
  - Root signing
  - Early TLD operation
  - Larger consortium
  - Luxembourg and Vancouver workshops
- 2006
  - Early applications
  - General availability of software
- 2007 ...



Domain Name Hijacking



Headlines

- Panix.com was hijacked on 15 Jan 2005
  - action returned it after 48 hours
- Gaining Registrar and Reseller at fault
- The problem is (also) systemic
- Other hijackings
  - hz.com is an equally compelling story
- Room for improvement

Tentative Recommendations

- Campaign for public awareness
  - Domain name risks and management of credentials
  - Domain name lock and auth-info mechanisms
  - Levels of service (contact hours, authentication techniques)
- Require Losing Registrar to send notification to the Registrant, in addition to Gaining registrar getting authorisation
  - Currently it's optional
  - Refinement of existing policy, not a reversal
- Development of emergency action channels
- Development of more visible enforcement
- Emergency "UnDo" procedure being pushed