

Security and Stability Advisory Committee

Open Meeting

Vancouver

November 29, 2005

Steve Crocker, chair
steve@stevicrocker.com



Topics

- Structure
- DNSSEC
- Domain Name Hijacking
- Alternate Roots



Structure

- Committee of roughly 20 experts
 - Volunteers
 - Key staff support
 - Broad participation across component constituencies
- Board committee
 - Advises ICANN board, staff, supporting activities
 - And the overall community



SSAC Members

- Alain Aina
- Jaap Akkerhuis
- KC Claffy
- Steve Crocker
- Johan Ihren
- Rodney Joffe
- Mark Kosters
- Allison Mankin
- Ram Mohan
- Russ Mundy
- Frederico Neves
- Jon Peterson
- Ray Plzak
- Mike St. Johns
- Doron Shikmoni
- Bruce Tonkin
- Paul A Vixie
- Suzanne Woolf



Others

- Dave Piscitello - ICANN Fellow
- Jim Galvin - Exec
- Daniel Karrenberg - Invited Guest
- Stefano Trumpy - GAC Liaison
- Patrik Fältström - IAB Liaison



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



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
 - ✓ Early TLD operation
 - ✓ Luxembourg and Vancouver workshops
- 2006
 - Early applications
 - General availability of software
 - Root signing
- 2007 ...



Domain Name Hijacking



Summary of Activities

- Sufficient headline incidents to merit SSAC attention
- SSAC investigation revealed many attack methods
- Room for improvement at all levels
- Major recommendations presented at Luxembourg
- Several recommendations already appearing in registration services

Alternative Roots and Registries



What are we talking about?



- Alternative root operators
 - An organization that operates root services and resolves TLDs outside the ICANN-sanctioned authoritative root
- Alternative registries
 - Organizations that register names in TLDs outside the delegation process sanctioned by ICANN
- Alternative root zone authority
 - Organization other than IANA that publishes a root zone
- Generically called alternate-roots or alt-roots

Types of alternative root operators and registries



- Compartmentalized (Isolated)
 - Private enterprise
 - Experimental
- Private Label (3rd level label) registries
- Commercial alternative root operators
- Protest alternative root operators
- Political



Private roots

- Operates within closed community
- Supports name schema and name service that has context within that organization
- Isolated from authoritative DNS
- No threat to single authoritative root name



Experimental roots

- Operates within closed community
- Supports a name schema and name service for research and experimentation
 - Next generation Internet Protocol test beds
 - International languages and character sets in top level domain labels
- Isolated from authoritative DNS
- No threat to single authoritative root name service



Private label registries

- Offer 3rd level domain labels under STLDs registered in a gTLD
 - E.g., registration of labels under US.com, UK.com ...
 - Name resolution does not affect authoritative DNS
- Operate below TLD, not accredited by ICANN
 - Use 2nd level labels that correspond to ccTLD labels
 - Labels were registered prior to addition of **Appendix K** to ICANN's unsponsored registry agreements



Issues with Private Label Registries

- Private labels that embed alpha-2 codes in 2nd level labels under .COM are confusing
 - Easy to confuse UK.com with com.UK
- Potential for deception and abuse
 - Can be used to divert users from intended destinations (phishing)



Commercial roots

- Regard TLDs as a potentially lucrative business
- Perceive ICANN accreditation process as a business impediment or unnecessarily constraining
- Philosophical difference?
 - no limits should be imposed on the creation of TLDs,
 - approval process for registry operators should be as simple as creating a corporation
 - the market will decide
 - *caveat emptor* applies



Business model Issues

- Alternative roots and registries
 - Do not engage in the traditional community or consensus process
 - Bypass ICANN accreditation criteria
 - TLD creation does not undergo the external and community scrutiny and evaluation
- Is this a philosophical issue?
 - Are *caveat emptor* and “market checks and balances” a good model for Internet name services



Technical issues

- Domains registered under alt-roots are not resolved to IPv4 and IPv6 addresses using conventional DNS client software and user configuration
- BUT users and DNS clients must be able to resolve names from both the authoritative DNS and each alternate root



Resolving alt-root names

- “Solutions” in the field...
 - Persuade ISPs and Internet users to replace the pre-stored IP addresses of the authoritative root name servers with alternate root server IP addresses
 - Persuade DNS operators to install a special, “expanded” named.root or hints file
 - Persuade Internet users to use specific DNS servers that can resolve authoritative and competing domain names
 - Develop downloadable extensions (browser plug-in)



In practice

- Users can't resolve names from authoritative DNS and multiple alt-root operators
 - Reconfiguration/reboot required
 - modify hosts file
 - Conflicting (competing?) software installation
 - Example: same autolocation software used by two alt-root operators, not possible to resolve TLDs from both
- Duplicate TLD labels exist (XXX)
- Root zone composition is typically union of authoritative root plus *one* alt-root
 - No way to coordinate and publish the uber-root zone file



Politically motivated roots

- Reasons to create “breakaway” roots include
 - Governance
 - Trust
 - Reliability, availability, fair allocation of cost and resources
 - Multilingualism
 - “Romance language” TLDs in ASCII (e.g., .viaje, .jeu, .ciao)
 - International character sets in the DNS (e.g., Chinese, Arabic)
 - Non-Latin scripts



Prospects for Alt-roots

- Private and experimental alt-roots are appropriate
- Commercial alt-roots have yet to prove themselves in market
- Support for non-Latin scripts and International character sets in the DNS are most viable of alt-root motivations
 - Are they a temporary forcing function for ICANN or a permanent fixture?
 - If the latter, how do we create seamless name resolution?