“Security” related proposals in the DAG v3

Jay Daley.nz
Agenda

- Background
- Mitigating Malicious Conduct
- High Security Zones
- HSTLD working group
Background

- Draft Application Guidebook v3
  - Two memoranda
- Mitigating Malicious Conduct
  - All new gTLDs MUST do
- High Security Zone Verification
  - Optional program for new gTLDs only
  - Also called HSTLD
  - ICANN working group set up to discuss
Context

- Security is in daily news
- High profile attacks common
- ICANN in awkward position
  - In a central position of influence
  - Under threat from ITU
  - Must be seen to do something
- ccTLDs cannot be in a bubble
  - This may apply to us some day

Nairobi ICANN, March 2010
Analysis

From my work in RISG
Registration Infrastructure Safety Group
www.risggroup.org

Group made up of
gTLDs
ccTLDs
Registrars
Security Companies
Vetted Registry Operators

- Already ‘bad actors’ running registrars. Prevent same at registry level.
  - Vetting of people/company bidding
  
- Generally a good idea

- BUT
  - Mere involvement in legal cases disqualifies
  - No mention of change of control
  - No prevention of gaming with multiple companies
Require DNSSEC

- Must go live with DNSSEC
- Huge boost for DNSSEC
- Generally a good idea
- **BUT**
  - Current gTLDs/ccTLDs don’t have to
  - Root zone scaling study points at possible issues from doing too much at once.
Prohibition on wild carding

ICANN board has already voted on for existing TLDs

Uncertainty as to how that will be implemented

Another good idea

BUT

Board recommendation came SSAC route - not a community consultation process
Thick WHOIS

- Good idea
- **BUT**
  - Gives better **access** not better **quality** of data
  - ICANN can insist on any other protocol
  - Thin WHOIS is not policed properly so what can be gained by doing that?
Central Zone File Access

- Not a good idea
  - No diversity of security/vetting
  - Few ccTLDs allow this, for good reason
- BUT
  - Security companies say it is vital
- New ICANN WG for this
  - Zone File Access
  - Has draft recommendations out
Abuse contacts and policy

- Three parts
  - Publication of abuse contacts
  - Mandated abuse policies
  - Publication of abuse policies

- Contacts good idea, rest not
  - What is so special about abuse policies?
  - Not in scope for ICANN to determine
  - Others are better at setting policies
Expedited registry request

- Where registry asks ICANN for contractual compliance relief
- Good idea
- BUT
  - No details on how provided
  - Or what threats will qualify
High Security Zones

- Voluntary program
  - Certification with onsite seal
  - New gTLDs only

- Wide scope
  - General IT and data security
  - Registry specific IT and data security

- Quite a messy document
  - Breakdown into topics presented here is not apparent in the document
General IT security

Includes

“Security management”
“Personnel security”
“Physical access control”
“Data collection, use, retention, access, etc”

BUT

Already plenty of standards - ISO 17799
Reinventing the wheel
Registry specific IT security

Includes

“Name resolution service management”
“DNSSEC deployment plan”

BUT

What existing registries agree on these?
What makes security special from other operational practices of a registry? (i.e. why no overall registry quality mark?)
Registry performance

Includes

- “WHOIS service availability”
- “WHOIS service performance level”
- “WHOIS service response times”

BUT

What has this to do with security?
Verification of registrant

◊ Yes, this is verification of identity for registrants of new gTLDs

◊ BUT

◊ Completely out of scope for ICANN
◊ Identity fraud already used extensively in bad registrations
◊ Breaks entire gTLD business model
◊ Break “equal access requirements”
Verification of entitlement

Quote is

“Other considerations, such as controls to address intellectual property concerns, could be added as components for future consideration in the lifecycle of this program”.

Not a security issue

Worrying to see it included
Registrant/Registrar interface

- Great idea
- BUT
  - Out of scope for ICANN
  - Prevents registrar differentiation
  - All domains are not equal
  - Same problem of equal access requirements
Summary

- Good discussion - odd venue
- Some big issues
  - Change in ICANN scope
  - Disregard for GNSO policy process
  - Lack of empirical evidence
  - Unclear market impact
  - Restricted scope
- But lots for us to think about
Any questions?

jay@nzrs.net.nz