High Security Zone Top Level Domain Program Workshop

High Security Zone Top Level Domain Program Advisory Group

HSTLD Workshop

11 March 2010

HSTLD Program – What is it?

The goal of the High Security Zone Top Level Domain Advisory Group is to bring together community representatives to evaluate the viability of a voluntary program, supporting control standards and incentives that could potentially be adopted to provide an enhanced level of trust and security over the baseline registration-authority controls.

- Designed to provide structured approach to improve internet community trust
- Help improve overall security of domains registered within TLDs that volunteer to participate

HSTLD Program – The Problem Statement

Certain individuals/organizations have sought to exploit vulnerabilities within the DNS technology, and the business practices of certain registration authorities, for inappropriate and/or illegal purposes. The exploitation of these vulnerabilities has threatened the security and stability of the Internet, and negatively impacted the trust users have when using the Internet.

There are several interested parties:

1. *Registrants would like to be sure that the name they register doesn't get hijacked through registrar/registry/their-own account compromise. (Including DNS, WHOIS, etc)*

HSTLD Program – The Problem Statement Cont.

2. *Registrars would like to be able to give reasonable guarantees to Registrants that #1 won't happen because they have controls. In order to do so, they require both Registrant and Registry cooperation*
3. *Registries would also like #1, and this requires the cooperation of Registrant and Registrar*
4. *End-Users would like to know that when they type in a given domain name, or navigate from a bookmark, etc. that they go to the right domain, and that the DNS, etc. hasn't been hijacked*
5. *End-Users would like to understand that a domain name registered within a particular gTLD is subject to registration standards, policies and procedures that are aimed at reducing malicious conduct by such registrants*

HSTLD Program – Who Might Volunteer?

- TLD operators wishing to establish and advertise an established control environment

- TLD operators that do not wish to advertise a control environment but wish to build an internal control model based on community standards

Origins of the HSTLD Advisory Group

- Focusing on security and controls is part of the ICANN new gTLD process
- Applicant Guidebook 2 and comments during and after the Sydney meeting The financial services community and numerous ICANN SSAC reports highlighted the desire for greater security controls
- Applicant Guidebook 3: initial concept paper published titled “A Model for a High Security Zone Verification Program”
- November 2009: call for volunteers to serve on an Advisory Group to continue developing initial concept

Tasks before the Advisory Group

- Continue to develop or improve upon concepts introduced in original concept paper
- Gather community input and feedback on proposed program
- Identify the issues
- Propose potential solutions
- Create a recommendations paper

Members of the Advisory Group

- Registries
- Registrars
- Internet security companies
- Financial institutions
- Law enforcement
- Legal professionals
- Knowledgeable individuals
- ICANN staff

- Co-chairs:
  - Michael Palage, Pharos Global
  - Christophe Reverd, Auditia

HSTLD Program Key Components

- Control Standards
  - Defined through Principles, Objectives, Criteria and Illustrative Controls
  - Established through effort of HSTLD AG
  - Available for community review and comment
- Demonstration of controls
  - Report card
  - Certification “Seal”
- Publication of participating TLDs

Control Standards

- HSTLD controls presented in ICANN's proposed strawman are being evaluated by the HSTLD AG
- HSTLD controls defined through structure of guiding Principles, Objectives, Criteria and Illustrative Controls
- Provide foundation of HSTLD program
- Current draft addresses controls for Registry, Registrar and Registrant

Control Standards - Principles

- PRINCIPLE 1: The Registry maintains effective controls to provide reasonable assurance that the security, availability, and confidentiality of systems and information assets supporting critical registry IT (i.e., registration services, registry databases, zone administration, and provision of domain name resolution services) and business operations are maintained by performing the following:
  - defining and communicating performance objectives, policies, and standards for system and information asset security, availability, confidentiality, and privacy;
  - utilizing procedures, people, software, data, and infrastructure to achieve defined objectives in accordance with established policies and standards; and
  - monitoring the system and information assets and taking action to achieve compliance with defined objectives, policies, and standards.

Control Standards – Principles Cont.

- PRINCIPLE 2: The Registry maintains effective controls to provide reasonable assurance that the processing of core Registry functions are authorized, accurate, complete, and performed in a timely manner in accordance with established policies and standards. The identity of participating entities is established and authenticated.

- PRINCIPLE 3: The Registry shall maintain effective controls to provide reasonable assurance that the processing of core Registrar functions by its Registrars are authorized, accurate, complete, and performed in a timely manner in accordance with established policies and standards. The identity of participating entities is established and authenticated.

Control Standards – Principles Cont.

- PRINCIPLE 4: Registrants in a High Security Zone are expected to maintain current and accurate information, and to commit to refrain from activities designed to confuse or mislead the Internet-using public.

- Work continues on evaluation and development of Principles, Objectives, Criteria and Illustrative Controls

Demonstration of Controls

- Provide basis for TLDs to participate in the program
- Current models include certification “seal” and self-assessment “report card”
- Each model has advantages and disadvantages
- Models are not mutually exclusive

Demonstration of Controls – Certification

- Certification defined within original concept paper as a “verification” process
- Establishes controls necessary to achieve certification
- Approved assessors measure certification controls and provide control assessment report to entity granting a seal
- Seal published for community advertisement and review
- Regular re-assessment of controls by approved assessor necessary to maintain seal

HSTLD Control Reporting – Report Card

- HSTLD AG recently introduced “report card” option
- TLD registry operators “self assess” implementation of HSTLD control standards
- Report card is matrix of HSTLD control standards against participating TLD registry operators
- Each control “graded” by TLD operators

HSTLD Control Reporting – Report Card Cont.

- Current report card grading model based on color code system:
  - White/Blank Box: Registry operator has provided no data in connection with specified control element.
  - Yellow Shaded Box: Registry operator has "self certified" their compliance with specified control element.
  - 50% Green Shaded Box: Third party has verified registry's compliance with specified control element at a point in time
  - 100% Green Shaded Box: Third party has verified registry's compliance with that control element over a period of time
  - Red Shaded Box: Registry found to be in noncompliance with a control previously reported as yellow or green. Potentially a violation of the registry agreement and may have compliance implications

Publication of Participating TLDs

- Provides method for public advertisement and assertion of controls for participating TLDs
- Value established through community understanding and acknowledgement of participating TLDs
- Publication could occur on individual sites and systems within a participating TLD
- Could be integrated into centralized dashboard
- Authenticity of certification or report card could be validated using a centralized system of record

Next Steps for the HSTLD Program

- Today: further discussion of the Concept Paper and development snapshot
- Next Steps for the Advisory Group
  - Continue to evaluate and develop Principles, Objectives and Criteria
  - Obtain feedback on HSTLD “report card” and “certification” models
  - Identify additional program components such as
    - Assessor requirements
    - Marketing and awareness
  - Contribute an HSTLD option paper to the next version of the Draft Applicant Guidebook
- Resources
  - HSTLD page: http://www.icann.org/en/topics/new-gtlds/hstld-program-en.htm

Thank You!

Questions and Discussion