DSSA-WG

Progress Update

Dakar – October 2011

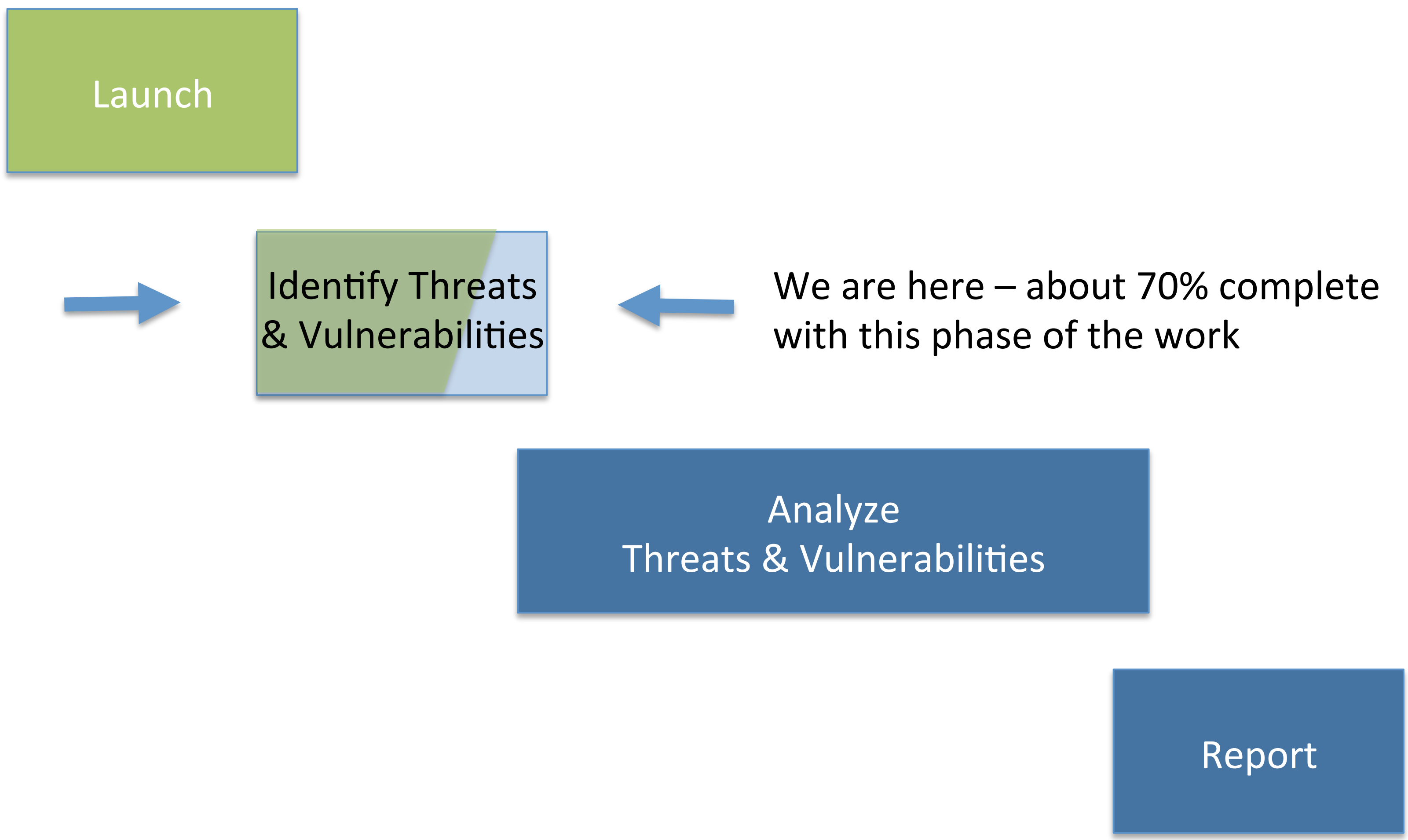
Charter: Background

- At their meetings during the ICANN Brussels meeting the At-Large Advisory Committee (ALAC), the Country Code Names Supporting Organization (ccNSO), the Generic Names Supporting Organization (GNSO), the Governmental Advisory Committee (GAC), and the Number Resource Organization (NROs) acknowledged the need for a better understanding of the security and stability of the global domain name system (DNS). This is considered to be of common interest to the participating Supporting Organisations (SOs), Advisory Committees (ACs) and others, and should be preferably undertaken in a collaborative effort.

Goals for today

- Update you on our progress
- Raise awareness
- Solicit your input

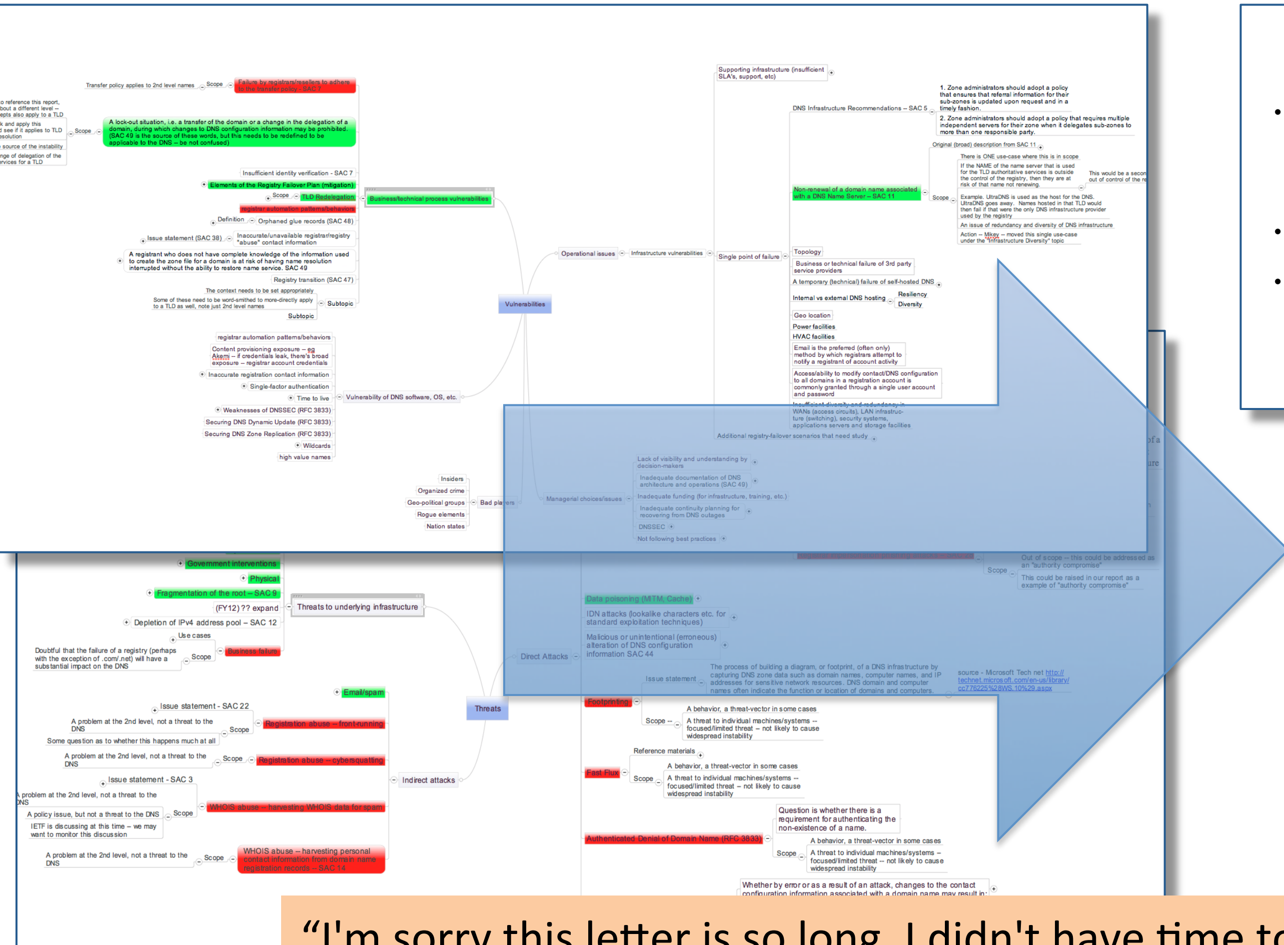
Approach and status



Activity since Singapore
Identify Threats

- The working group has:
  - Developed lists of vulnerabilities and threats (with definitions)
  - Made preliminary choices about which threats are in/ out of scope for analysis
  - Developed preliminary criteria and mechanisms for segregating sensitive information
- Remaining work in this phase
  - Solicit additional lists/definitions from other experts and interested parties
  - Arrive at a final (prioritized) list of threats and vulnerabilities

Brainstorming and refining



Threats to underlying infrastructure
(Draft – for discussion only)

- In scope
  - System failure
  - Governmental interventions
  - Physical
  - Fragmentation of the root
- Under discussion
  - Depletion of IPv4 address pool
- Out of scope
  - Busin… regist… have a…

Threats – direct attacks
(Draft – for discussion only)

- In scope
  - DDOS – distributed denial of service
  - Packet interception
  - Recursive vs authoritative nameserver attacks
  - Data poisoning attacks
- Under discussion
  - IDN attacks (lookalike characters for standard exploitation techniques)
  - Malicious or unintentional alteration of DNS configuration information
- Out of scope
  - Footprinting
  - Authenticated denial of domain name
  - Malicious or unintentional alteration of contact information
  - Rationale:

Threats – indirect attacks
(Draft – for discussion only)

- In scope
  - Email server-hopping under IPv6 (causing collateral damage due to load)
- Out of scope
  - Registration abuse – front-running
  - Registration abuse – cybersquatting
  - WHOIS abuse – harvesting WHOIS data for spam
  - WHOIS abuse – harvesting personal contact information from domain name registration records
  - Rationale:
    - These are problems at the 2nd level, not a threat to the DNS
    - In some instances these are policy issues that do not threaten the DNS
    - In some cases the IETF is discussing the issue and we will monitor that discussion

> "I'm sorry this letter is so long, I didn't have time to make it shorter."
>
> — *George Bernard Shaw, Pascal, Goethe, Wilde, Cicero, DSSA*

Scope

- From our charter, “the working group should focus on "The actual level, frequency and severity of threats *to the DNS*.... The DSSA-WG should limit its activities to considering issues *at the root and top level domains* within the *framework of ICANN’s coordinating role* in managing Internet naming and numbering resources as stated in its Mission and in its Bylaws.”
- The WG refined this to add “we are *not* to look at every threat having to do with, or taking place via, the DNS, or that impacts some party using the DNS. *We are concerned with “the” DNS, i.e. threats to the system itself, and relevant to ICANN’s role.*”

Threats to underlying infrastructure

(**Draft** – for discussion only)

- In scope
  - System failure (e.g. hardware/software failures, etc.)
  - Governmental interventions (e.g. seizure, blocking, etc.)
  - Physical events (e.g. natural disasters, etc.)
  - Fragmentation of the root (e.g. alternate roots, root scaling, etc.)
- Under discussion (**your thoughts?**)
  - Business failure
- Out of scope
  - Depletion of IPv4 address pool
  - Rationale:
    - The concerns (routing table growth and route fragmentation) will happen anyway
    - The DNS is not a heavy consumer of IP addresses, thus depletion is unlikely to have a significant impact

Threats – direct attacks

(**Draft** – for discussion only)

- In scope
  - DDOS – distributed denial of service
  - Packet interception
  - Recursive vs authoritative nameserver attacks (e.g. using vulnerable recursive DNS servers as reflectors to attack TLD DNS servers)
  - Data poisoning attacks
- Under discussion (**your thoughts?**)
  - IDN attacks (lookalike characters for standard exploitation techniques – awaiting results of the Variants project)
  - Malicious or unintentional alteration of DNS configuration information
- Out of scope
  - Footprinting
  - Authenticated denial of domain name
  - Malicious or unintentional alteration of contact information
  - Rationale:
    - These are behaviors or, in some cases, threat vectors
    - These are focused/limited threats, not likely to cause widespread instability

Threats – indirect attacks

(**Draft** – for discussion only)

- In scope
  - Email server-hopping under IPv6 (causing collateral damage due to load)
- Out of scope
  - Registration abuse – front-running
  - Registration abuse – cybersquatting
  - Registration directory service abuse – harvesting registration data for spam
  - Registration directory service abuse – harvesting personal contact information from domain name registration records
  - Rationale:
    - These are problems at the 2nd level, not a threat to the DNS
    - In some instances these are policy issues that do not threaten the DNS
    - In some cases the IETF is discussing the issue and we will monitor that discussion (harvesting registration data for spam)

Vulnerabilities
(**Draft** – for discussion only)

- Operational issues
  - Infrastructure vulnerabilities (e.g. single point of failure, DNS software vulnerabilities, insufficient SLA's etc.)
  - Business and technical process vulnerabilities (e.g. orphaned glue records, lock-outs, TLD redelegation, etc.)
- Registry failure and continuity
- Managerial choices/issues
  - Not following best practices (e.g. measures to detect/prevent unauthorized changes, etc.)
  - Gaps in continuity planning (e.g. responsibilities, actions, documentation, etc.)
  - Inadequate funding/resources (for infrastructure, training, staff, etc.)
  - Lack of visibility/understanding by decision-makers

Questions?

- This “scoping” work is well along, but not complete. We are interested in your thoughts