DNS Security, Stability and Resiliency

John Crain
Chief Technical Officer

April 21st 2009

Garmisch

Agenda

- The Global DNS SSR Symposium
- Problems and Opportunities
- Questions?

The Organization

- Sponsors:
  - Georgia Tech, DNS-OARC, George Mason University, ICANN
- Chairs:
  - Dave Dagon, Georgia Tech
  - John Crain, ICANN

Global DNS Symposium

- Feb 2-3 2009, Atlanta, Georgia
- 100+ invited experts
- Attendees from many sectors
  - Registries
  - Registrars
  - Security Agencies
  - ISPs
  - DNS software manufacturers
  - OS/browser manufacturers
  - Hardware Suppliers
  -

Goal of Symposium

- Main purpose was to document known risks to the DNS and to perform a gap analysis on current work and solutions.

- Further to define areas where collaborative solutions may exist.

  – http://www.gtisc.gatech.edu/icann09

Focus areas

- Enterprise use of DNS
- DNS in resource constrained environments
- Combating malicious use of the DNS

Understanding Risks

- When talking about Risk one of the first things we realized.....

- *"The level of awareness with respect to the DNS is very low"*
  - *All quotes from Symposium Report*

Problems

&

Opportunities

Problem:

- There is a need for training across all sectors of the industry to raise both skills and awareness.

- *"Operators and managers from the smallest ccTLD to large service providers require training to increase skill and capacity in operating and defending the DNS"*

- The issue came up in all three sub-groups!

Opportunity:

- ICANN has been active in promoting training for CcTLD administrators.
  - Technical workshops together with organizations such as ISOC and the NSRC.
  - Working with regional TLD groupings to train on Contingency Planning.

- **How do we improve in other areas of the industry?**
  - Who should be doing this type of awareness/skill raising?

Problem:

- There is need for better coordination!

- CERT's are not as well known in the operational community as we would have hoped.

- *"The DNS technical, operational, and security communities are disjointed and in need of a dedicated information sharing and incident response capability"*

Opportunity:

- Recent needs to coordinate against conficker have raised awareness in the community.
- Discussions will be held at ICANN Sydney in June.
- How do we bridge the gap between the CERT world and the DNS world?
- Awareness is first step to a solution?

Problem

- “the toolset, both technical and non-technical must improve; operators need simplified technical tools, managers need ways to conduct operations proactively and the community as a whole needs accountability standards and methods for measuring those standards”

- There are very few affordable tools available that focus on DNS operations.

Opportunity:

- There would appear to be a market for such tools.
- How can we as a community make developers aware?
- Are there things that can be done to encourage specific open-source tools?
- Who can champion this cause?

Problem

- *"concerns were expressed over organizational outsourcing of DNS services based on an incomplete review of information which didn't account for potential reductions in control, visibility, privacy and internal know how"*

- The underlying issue seemed to be about making informed decisions rather than outsourcing per se.

Opportunity:

- Training programs such as those held by ICANN, ISOC and NSRC will hopefully increase DNS operators ability to make informed decisions.
- Are there other things that could/should be done?
- If so by whom and how?

Problem:

- “clearer understanding is needed of ICANN’s mission and role with respect to security, stability and resiliency of the DNS and the Internet at large.”

- There was a wide divergence on what people thought ICANN’s role was or should be.

Opportunity

- – ICANN will publish a document soon that will hopefully bring clarify to what ICANN’s role is, and as important “is not” with respect to the Security, Resiliency and Stability of the Internet”

The whole report

- *“It is a fact that there are many threats associated with the use of DNS including lack of authentication, cache poisoning, DDOS etc. However often it can be simple and less complicated issues that are the root cause of failures. Lack of awareness of the importance of DNS and not planning accordingly can cause equally catastrophic results.” - John Crain*

- Please read the report!

More importantly

- When reading the report please think about possible ways of becoming part of the solution.
- Being more aware is a good start but maybe you can also help with specific issues?

Thank You