The Global DNS
Security, Stability, & Resiliency Symposium
February 2009 - Atlanta, Georgia, USA

Summary, Trends, and Next Steps

April 2nd, 2009

Intended Purpose

This report is a collaborative effort and based on the accumulation of thoughts, opinions, and ideas expressed at the Symposium; it does not represent any particular individual's or organization's opinion. The Symposium steering committee has validated this report as an accurate representation of the discussions and recommendations for further study from the Symposium. This report will be used as a basis to guide further work in this area.

Executive Summary

The Symposium was the first of its kind to bring together cross-functional stakeholders to address risk to the DNS. The Symposium's three breakout sessions focused on risks from different perspectives: enterprise use, resource constrained environments, and combating malicious use. Attendees from a range of backgrounds contributed their thoughts to the risks, current efforts, and potential solutions within each session. Several common themes emerged from the discussions.

First, the level of awareness with respect to the DNS is very low; consumers of DNS services, from end-users to large enterprises do not realize their use of and reliance on the DNS. Operators and managers from the smallest ccTLD to large service providers require training to increase skill and capacity in operating and defending the DNS. Second, the DNS technical, operational, and security communities are disjointed and in need of a dedicated information sharing and incident response capability. These functions are generally performed by CERTs, but no such capability exists expressly for the DNS community. Third, 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. Fourth, 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". Finally, 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. Two camps clearly exist here, one in favor and one against expanding the leadership and operational role ICANN plays.

To capitalize on the results of the Symposium, a collaborative structure is necessary to set priorities, establish goals, select implementation teams, initiate work and measure progress. Each breakout session brainstormed potential solutions and questions for additional study. Specifically, a DNS collaborative response, awareness, technical training, and future DNS security, stability, and resiliency collaboration should take precedence within the issues selected for further study and implementation.

CONTENTS

Global DNS SSR Symposium Summary, Trends, & Next Steps

1. Introduction

The Global DNS Security, Stability, and Resiliency Symposium sought to involve participants from a wide range of areas to collaborate on cross-functional solutions to DNS risks. The Symposium was envisioned to present, integrate and expand on previous work, with the goal of understanding the underlying risks, identifying relevant stakeholders, collaborating on potential solutions, conducting a gap analysis between risks and solutions, and building a cross-functional strategy to address root causes of DNS risks. Participation in the Symposium was by invitation only, and technical, operational, security, policy, and law enforcement / government perspectives were represented by those in attendance.

Three areas were selected to focus the Symposium discussions, 1) understanding enterprise DNS reliance and enabling effective risk mitigation (referenced herein as Enterprise Use); 2) meeting challenges to secure & resilient DNS operations in resource constrained environments (Resource Constrained Environments); and 3) identifying and improving collaboration in combating malicious activity leveraging the DNS (Combating Malicious Use). The goals of each session were to build understanding of the focus area, identify current approaches and the actors involved in those approaches, identify gaps between current approaches and what's needed, and brainstorm possible solutions and potential actors to fill those gaps.

2. Breakout Session Overview

The Symposium featured three separate breakout sessions, each focusing on a different risk area to the DNS. Each attendee was asked to select and participate in one breakout session during the Symposium. A mid-Symposium review and a final presentation (both during plenary sessions) for each of the breakout sessions provided all attendees an overview of the activities regardless of which session they chose to participate in, as all sessions ran concurrently. The breakout sessions discussed gaps in knowledge, cross-functional collaborative opportunities, and examined coordination, operations, and policy solutions in addition to technical solutions to particular issues affecting the DNS.

The Enterprise Use breakout session discussed current enterprise awareness of, reliance on, and risk mitigation with respect to the DNS. Prior to the Symposium, it was posited that most enterprises have a number of internal operational or external dependencies on the DNS, but have little or no awareness of their dependence on the DNS for mission critical operations. The session sought to understand the extent of enterprises' DNS reliance and ways to increase awareness within that community.

The Resource Constrained Environments breakout session discussed the challenges of secure and resilient DNS operations in resource constrained environments. Prior to the Symposium, it was posited that DNS operations pose unique challenges in environments where limited bandwidth, high latencies, unreliable equipment environments, limited budgets, and limited personnel are the norm. The session sought to identify cross-functional ways in which resource constrained operations could move from a reactive stance to more secure and resilient operations via proactive means.

The Combating Malicious Use breakout session discussed ways of identifying and improving collaboration in combating malicious activity which leveraged the DNS. Prior to the Symposium, it was posited that the DNS is used in unintended ways (from a standards perspective) to facilitate or

magnify malicious acts. The session sought comprehensive, cross-functional approaches to addressing the risks associated with this activity.

On the afternoon of the second day, the Enterprise Use and Combating Malicious Use sessions were combined into one session. Several common themes were seen between the two sessions, and a combined discussion yielded thoughts that the two groups had not considered separately.

3. Common Themes Among Breakout Sessions

This section presents the issues that were found, through after the fact analysis, to be common to all of the breakout sessions.

3.1. Awareness & Skill Training

The single unifying theme among all three sessions was the lack of awareness and skill with respect to the DNS. Unfortunately, the DNS works well enough most of the time that an economic mandate or other incentive is not there to increase awareness which makes this a challenging problem.

Awareness extends from end-user education to the need for enterprise contingency plans to account for DNS reliance. Technical skills training in both day-to-day operations and incident response are generally viewed as lacking across the board. Today's efforts in both awareness and technical training are viewed as ineffective as no follow-up or mentoring occur post-training. Training should be viewed as more than just a class and should focus on the "WHY", not just the "HOW-TO" in order to build more effective human capital. Improved awareness and technical training benefits everyone from enterprises, who can grasp and mitigate risks associated with their use of the DNS, to small ccTLD registries, who can offer more stable operations.

Each breakout session summary highlights areas for improvement within awareness and skills training, but many of the concepts and topics are applicable regardless of organization, be it small registry or large enterprise.

3.2. Improving Information Sharing and Incident Response Capabilities

Information sharing within the DNS community is sorely lacking and related to that, incident response procedures, capabilities and capacity to detect, respond and defeat malicious activity are limited at all levels from root operators, to registries, to service providers, to end users.

A clear need was established for a centralized method of exchanging information, be it indicators of malicious activity, or a business continuity plan template for ccTLDs. Currently, it is professional networks that facilitate information sharing; and a trusted, common ground, where operators, researchers, law enforcement, policy makers, and other stakeholders can connect with each other is desired.

For incident response procedures, enclaves may have their own established procedures, but many more have not and sharing of those procedures would increase the net sum capacity of the DNS community to defend itself. There are no well-publicized best practices for incident response expressly related to the DNS, no common measures of success, and no established exercise program to validate an organization's detection and response capabilities.

CERTs worldwide perform similar functions, but there is no community of practice devoted to the DNS as of yet. Additional details, as relevant to each session, are provided in the "Solutions and Possible Actors" within the breakout summary.

3.3. Improved Tools

The DNS community is in need of better "tools", both technical, and non-technical.

From the technical perspective, DNSSEC suffers from deployment issues and while DNSSEC-in-a-box efforts are underway, most organizations see DNSSEC implementation as a major challenge. Within resource constrained environments, open source tools are de rigueur, but incident response and monitoring tools are generally viewed as under developed.

On the non-technical side, trusted metrics for ensuring quality and grading do not exist. There is a perceived lack of accountability standards and the ability to measure such standards even if they did exist. Templates for contingency response plans, incident response procedures (see above), and awareness training (see below), are vital to organizations seeking to take a proactive stance in security, stability, and resiliency.

Recommendations for "tool" improvement are provided in the "Solutions and Possible Actors" section within each breakout session summary.

3.4. Outsourcing Concerns

A smaller thread emerged from the sessions over outsourcing of technical services (e.g. authoritative name resolution, Anycasting, network monitoring, etc) and the concerns it raises within enterprises and resource constrained environments, and the impact it has on combating malicious use.

There are both pros and cons to outsourcing, and it's imperative that organizations considering outsourcing understand both sides. Generally, a decision to outsource is resource (time, manpower) based, and the second order effects on security and stability are not reviewed. From the resource constrained environment session, outsourcing was seen to provide a low initial investment, instant access to expertise, and diversity, but at a loss to internal "know how", control, visibility, and privacy. Such decreases may open the door to increased malicious use.

3.5. ICANN Mission & Role

Common among all three sessions was a desire to understand ICANN's role with respect to security, stability and resiliency of the DNS. Very clearly, two camps emerged within the sessions, one in support of ICANN's involvement and even for expanding involvement, and one vehemently against it. Arguments against cited mission creep, ICANN's ability (or lack thereof) to focus on issues, and its presumed desire to not be a leader/owner within the community. Proponents of expanded involvement sought ICANN to provide strategic leadership, facilitating collaboration within the community, and connecting key stakeholders for a wide variety of reasons ranging from incident response to research. Focus areas for ICANN involvement included registry/registrar contracts and accreditation, policy vetting, awareness and outreach programs, funding, establishing priorities, setting goals, and progressing programs towards those goals. The "Solutions and Possible Actors" section of each breakout session provides specific actions where ICANN was suggested as a solution provider.

4. Breakout Session Specific Results

This section presents a summary of the discussions that were specific to each breakout session. Each session attempted to avoid technical details and stay at a high enough level to ensure multiple perspectives were considered.

4.1. Enterprise Use

4.1.1. Discussion Summary & Recommendations

The Enterprise Use session sought to create a taxonomy of failure modes an enterprise might see in order to frame the discussion. Failures were separated into issues affecting confidentiality, integrity, and availability, and the ensuing discussion used examples of failures to identify the impact to each of the three areas.

Enterprises must consider each of the three areas (confidentiality, integrity, and availability) with respect to their authoritative and caching DNS infrastructures, be it in-house or outsourced. Failure to do so can expose the enterprises to risks, both common and uncommon. A table constructed from these discussions follows:

	Confidentiality	**Integrity**	**Availability**
Authoritative	Cracked DNSSEC Signing zone walking Private key exposure Loss of Privacy Disclosing data Business partners Loss of Control Social Engineering	Loss of Domain Name Control Court Action Registrar event Negligence Expiration Loss of Authoritative Server Configuration Error Server/Datacenter Failure DDOS/other attack Loss of a Specific zone Configuration error Server/datacenter failure Device caching bad data	
Recursive / Caching	Loss of Privacy Visible cache content Can leak data to net Allows for network 'walk'	Cache Poisoning Configuration Error Stale Data	Server down Server unresponsive External Dependency Misconfiguration Use external for internal names

Expanding on these, the legal risks associated with DNS "events" involve loss of domain through court action (intellectual property right challenges, revocation for malicious use or violation of registrar policies), collateral damage from anti-malware should a domain be associated with malicious use, and brand protection. Enterprises generally have little awareness regarding issues or events with registrars or registries, but must manage their registrar relationships and have good internal awareness of that relationship. Having someone aware of relevant national policies and regulations was suggested as a best practice. Further, good administrative policies and employing a skilled lawyer can aid in identifying and resolving legal risks.

With regard to registrar-related risks, enterprises are subject to social engineering and domain hijacking. Malware that specifically harvests registrar or registrant credentials or registrars with questionable policies exists – but enterprises may not be aware that they exist. Knowing where an enterprise's registrar is based, and making an effort to research registrars before selecting one with

good authentication methods (e.g. two-factor authentication), strong privacy and confidentiality policies, and other well documented policies were suggested as best practices.

Outside of this taxonomy, specific risks associated with phishing, DKIM and other keys in DNS, outsourcing, and standardization vs. diversity were discussed. Phishing attacks can be used to gain access to specific networks or single hosts, and spear phishing attacks targeting C-level executives have been seen. Phishing can be mitigated through continual user awareness and internal "phishing" exercises. When outsourcing DNS, the true costs are not well understood and security is usually an after-thought. Further, through standardization, organizations can reduce the number of DNS servers they have, which leads to monocultures of small number of operators and code bases which effectively limit diversity, which is a key capability in surviving DNS attacks.

With regard to tools, a set of sample policies and best practices as well as evolved technical toolset is highly sought after as there is a perception that too many seemingly random tools exist. Many failure modes within the DNS map to one ambiguous error code which does not aid in resolving issues. Enterprises are exhibiting a tendency to delay DNSSEC implementation until the root is signed with reasons such as "my competition isn't doing it", or ".COM is comparable to the root", or "insufficient resources (skill sets)", or "lack of DNSSEC-in-a-box implementations". Non-obvious answers to delay DNSSEC implementation involved possible legal liability, public perception, and a broad range of DNSSEC failure cases. Additionally, the separation of registries and registrars presents a decentralized structure, which makes DNSSEC implementation more difficult. Considering the case of an enterprise operating its own name servers, information must go through the registrar to get to the parent zone. The potential burden to quickly propagate this information may discourage registrars from implementing any mechanism to forward this information. Unfortunately, enterprises don't seemingly care enough to investigate DNS risks, and coupled with the expectation that "DNS always works", the challenge becomes getting them interested and aware of the issues and then enable them to address the issues within their organizations.

Enterprises need to develop contingency plans for loss of DNS as they currently do for other contingencies (e.g. power loss, weather disaster, etc). However, the lack of awareness of an enterprise's use of and reliance on the DNS is profound, and such contingency plans are unlikely to be established by most enterprises. The notion of "insurance" to guard against DNS outages was briefly discussed, but quickly dropped, as data on outages is scarce and certainly, no actuarial tables exist to establish the resulting risks and associated costs.

4.1.2. Open Questions

- Is there value in defining such a DNS risk taxonomy, and if so, where could it be used, and who could benefit from it?
- Can a more complete understanding of the risks resulting from the registrar, registrant, and registry relationship be further defined?
- Why did Sweden implement DNSSEC so willingly? Are there best practices and rationales that can be distilled from this to make the case for enterprise adoption of DNSSEC? If larger organizations adopt DNSSEC (e.g. GoDaddy, Network Solutions, etc) – will smaller organizations follow suit?
- Is a DNSSEC GUI implementation possible? Who would build such a thing?
- The Drill plug-in (NLNet Labs) supports DNSSEC at the application layer, but development has stalled. Would this type of tool assist or hinder efforts?

4.1.3. Solutions and Possible Actors

- Increase awareness of enterprise use of and reliance on the DNS; enable organizations to balance risks associated with its use.
- Evolution of the technical and non-technical toolset, or commercial products that do tasks effectively and affordably.
- Establish a direct channel between ICANN and registrars to allow for domain provisioning, protection, and security related matter (e.g. pre-registering domains based on reverse engineered malware)
- Augment the DHCP protocol to pass DNSSEC related configuration information to clients.

4.2. Resource Constrained Environments

This session sought to identify the challenges to security and resilient DNS operations in resource constrained environments. The task was separated into 1) defining a resource constrained environment, 2) understanding the core constraints, and 3) identification of the issues, solutions and potential actors within the solution space.

The session defined a resource constrained environment to be one in which limited financial resources, manpower, time, and generically, services, were available. The perspective of a country code Top Level Domain (ccTLD) organization was used to focus the discussions, but it was noted that resource constrained environments can exist anywhere, and notably in enterprises of any size. From a ccTLD point of view, it was posited that most issues with regard to secure and resilient operations were a result of operating in a purely reactive mode, not having the resources to accomplish tasks proactively. Problems that are not prioritized go unresolved as a result. A lack of knowledge, staffing, and engagement in and access to professional human networks were identified to be the causal factors of operating in a reactive mode, and the discussion of solutions and possible actors used these three areas to focus on how to empower an organization to operate proactively.

For completeness, other constraints were noted to be access to low cost tools, the relative cost of technology, sparse connectivity, inter-human communication (language, culture, political), regulatory, resistance to change, misaligned resources, and lack of stable network and communication infrastructure.

4.2.1. Discussion Summary & Recommendations

Knowledge

Within the knowledge constraint area, two themes emerged: 1) trained staff and 2) awareness / information sharing – both of which have an impact on an organizations ability to operate proactively.

Trained Staff

Technical operators without a solid background in DNS are charged with operating the DNS. Managers without a background in operations, security, or planning are charged with overseeing it. These gaps in knowledge are masked by the forgiving nature of the DNS, which often continues to work despite being misconfigured.

A trained staff operates more efficiently than an untrained one, and is able to provide information to drive organizational-level decisions. The challenge is to obtain quality training and tools to enable a staff, both technical and managerial, to perform operations efficiently. The current state of affairs for training results in a seemingly ad-hoc collection of

training, ranging from self-study, to friends, to conference workshops, to well-intentioned capacity building programs. E-Learning was specifically discussed and determined to dependent on both the student and the topic for its effectiveness and therefore, not generally viewed as an effective solution. The lack of structure results in "hit or miss" training that works for some, but not all, depending on the student. The ad hoc nature and a lack of monitoring and evaluation of these training programs have resulted in an inability to monitor their effectiveness.

To complicate matters, current training offerings suffer from shortcomings in both packaging and localization of material. Effectively packaged training introduces students to the "why" as opposed to the "how", and addresses the knowledge constraints of conducting operations proactively. It should provide students with experience and exposure, simulations, incident response drills, and templates to give them a head start within their organizations. Localization provides students with access to training in their native language through translation and interpretation as well as ensuring it's adapted or customized to the local environment.

Operators and managers that are well versed in security, incident response, and contingency planning are postured to operate proactively.

Information Sharing

Resources and information about DNS are spread far and wide across the World Wide Web, and a search for specific information increases demands on an operators already constrained time. Further, the cross-flow of information between ccTLDs seems to be limited to already well-established relationships and operators do not know where to being their search when seeking lessons learned and best practices from other ccTLD operators and organizations.

A common meeting ground was discussed as a possible solution to this problem; either stand-alone or connected to a CERT-like organization specifically for the DNS. In any case, a useful common ground is one that operators can find technical, operational, and business related information, best practices and lessons learned from trusted sources (other TLDs, vendors, CERTs, researchers) regarding the DNS without having to conduct large-scale searches and manually cull errant or misleading information.

Mentorship and exchange opportunities within the community may assist in increasing the net sum of knowledge. Language presents a challenge with exchange programs, but currently, no program exists to coordinate mentorships and exchanges between operators. As a result, these opportunities are limited to organizations with well established relationships.

Staffing

The access to and retention of qualified operations were seen as the primary concerns with respect to the staffing constraint. Hiring new, qualified people can be expensive, and a high rate of turnover (or churn) results in a constant influx of people within the organization, at increased hiring costs. Building and maintaining human capital can significantly affect an organizations ability to operate proactively as less time is dedicated to managing and training personnel.

A few organizations offer help during emergencies, and governments may contribute aid during exceptional times, but there is little assistance for staffing when operating under normal, day-to-day conditions.

Mutual aid agreements, internships, establishing hiring pipelines, and exchange programs were all discussed as possible solutions. Mutual aid agreements provide manpower (e.g. TLD A provides TLD B one staff member for a short period to accomplish a specific task), cross training opportunities, and technical assistance or backup capabilities (e.g. TLD A and TLD B host each other's secondary servers) provided two organizations have the ability to implement the agreements. Internships and hiring pipelines, established through local universities or schools, can provide low-cost labor that can be developed into knowledgeable full time staff. Structured programs like Geek Corps can provide assistance, but organizations must take into account the risks associated with amateur or unskilled volunteers.

Retention of staff was identified to be a large problem. A staff needs to be motivated by professional desire and pride in resource constrained environments, as monetary incentives for retention are not feasible. Further, an organization must plan and be prepared for the eventuality that staffs will change – effective project management (setting short term goals and defining tasks) can allow an organization to take best advantage of the people it has.

Professional Networks

Within the professional networks areas, it was determined that resource constrained organizations have difficulty establishing networks of professionals to reach out and solicit assistance from. An organization will instinctively turn to its professional network, either in reaction to an event / incident or for proactive assistance. It is imperative that organizations know where to begin establishing their networks.

Stakeholder awareness was discussed as a first step in establishing a professional awareness and is the notion of establishing relationships with an organization's direct stakeholders (governments, ISPs, registrars, CERTs, etc). This has the added benefit of educating those stakeholders as to the organization's importance.

Other possibilities included personal contacts, regional TLD groups, and networking at NOG or other conferences. Regional groups are successful because member organizations contribute to their success and the success of the other members. But what about organizations that are not members of regional groups for whatever reason (lack of funding, inability to travel, etc). As with information sharing, there is no central point to go to for assistance with building a network.

4.2.2. Open Questions

The following questions were brought up during the discussion and were unable to be answered or required additional research. They are mentioned here to preserve for and focus future efforts.

- Can a survey of ccTLDs be conducted capturing the following data?
  - People (Number, Skill set, Hiring Source)
  - Size (number of registrations, registrars, etc)
  - Revenue
  - Internal Training Programs
  - Professional Networks
  - Communication mechanisms with other ccTLDs

- How do other resource constrained organizations retain staff where monetary incentives are not feasible?
- Beyond current efforts, is there a better way to increase the number and quality of trained operators?
- Are there metrics or measurements that can be made to build information to drive monetary decisions with regard to diversity and capacity? (Current belief is that there is no substantial measurement data coming from resource constrained environments which could provide insight into future efforts)

4.2.3. Solutions and Possible Actors

The following actions and possible actors were particularly highlighted during the discussion. Additional ideas follow in the table summarizing all actions and actors with respect to solutions targeting knowledge, staffing, and building professional networks within resource constrained environments.

- DNS CERT – an organization devoted to security and resiliency of the DNS and act as a central clearinghouse for DNS information. Possible actors: ICANN, DNS-OARC, existing CERTs
- Capacity Building Programs – the notion of conducting technical and managerial training to resource constrained environments, focusing on efforts to allow organizations to operate proactively. Create templates for disaster recovery and incident response. Possible actors: ICANN, ISOC, NSRC, Larger TLD operators, Regional TLD groups
- Training & Testing Lab – would allow operators to test configuration changes without affecting their live networks, would preclude them from having to build their own test networks, and would allow operators to conduct training on realistic systems. Possible actors: ICANN, ISOC, NSRC, DNS-OARC.
- Information exchange and sharing platform – creation of a trusted, centralized point to exchange technical, operational, and business information. Could include mentorship and staff exchange listings, enabling information on building professional networks, and capacity training. Possible actors: ICANN, ISOC, NSRC, DNS-OARC, Regional TLD groups
- Raising Stakeholder Awareness – building awareness briefing templates and having ccTLDs meet with providers, governments, CERTs, registrars, etc, to build their professional networks and increase awareness of the organizations significance and "criticality"

Knowledge		Staffing		Professional Network	
Actions	**(Possible) Actors**	**Action**	**Actors**	**Action**	**Actor**
- (Regional) training	I*, vs	- Mentorship	ccTLD, LCs	- Regional (training)	I*, NOGs, vendors, ISPs, LCs, rsrar, CERTs,
- Localized material	Local community, Univ., Govs, NOGs, TLD, ds				
- Frameworks (BCP, templates, cookbooks)	I*, CERTs, NOGs, vs, TLD	- Scholarships	Univ., Govs, International organizations (World Bank)	- Creating platform (identifying)	TLDs, I*,NOGs, CERTs
- Trusted specialized Internet content (e-learning) sharing	I*, NOGs, vs, ds, TLD				

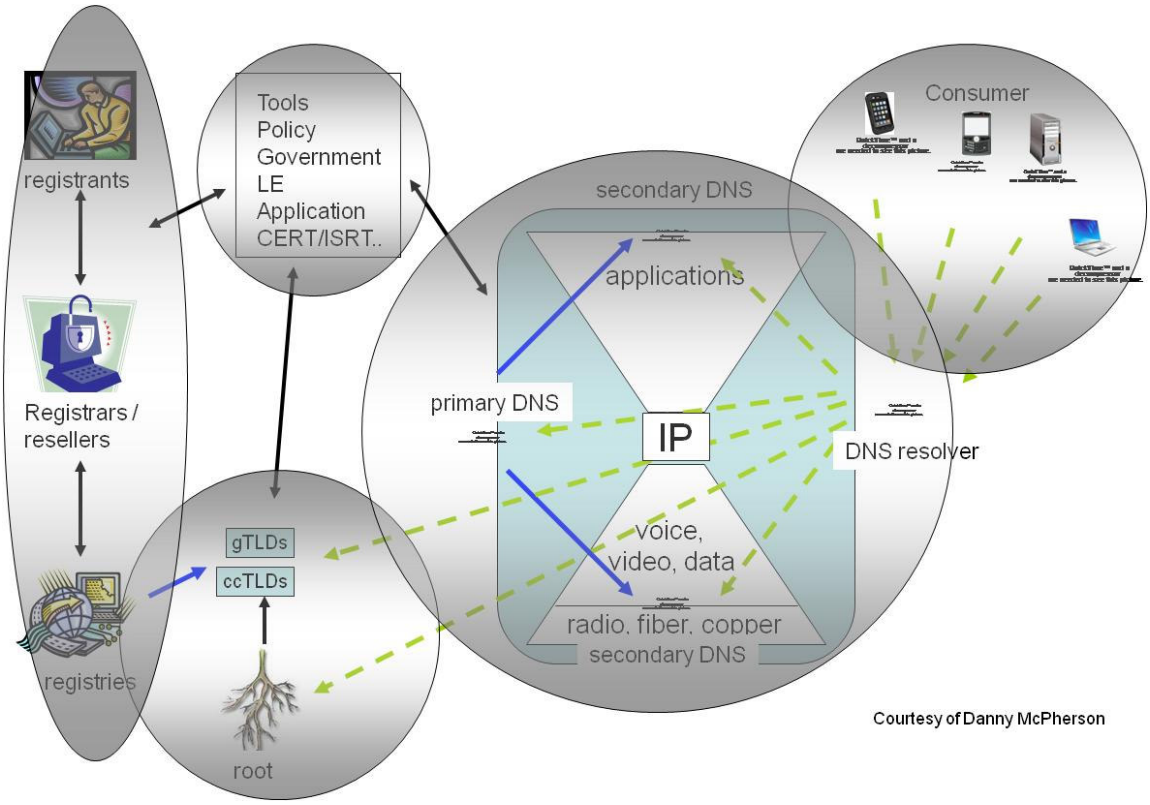
Knowledge		Staffing		Professional Network	
Actions	**(Possible) Actors**	**Action**	**Actors**	**Action**	**Actor**
-Packaging	Univ, TLDs, I*	- Internships	- Univ.	- Exposure	NOGs, I*, CERTs,
-Experience	Univ, CERTS, ccTLD				
-Exposure to issues	TLDs, CERTs, NOG, ccTLD, I*	- Awareness of criticality of staff	- ccTLDs, TLDs, NOGs, lobby, I*	- Collaboration frameworks	I*, TLDs, ccTLDs, Govs.
-Mentorship	ds, I*, Univ., LCs				
- Scholarships	I*, Gov, vs, NOG, Univ	- Staff retention	ccTLD	- Mentorship	Same as knowledge section
- (creating) Stakeholder awareness	ccTLD, I*				

Possible Actors (abbreviated name used in table):

- Vendors (vs)
- DNS experts (ds)
- NSRC/ISOC/ICANN (I*)
- Governments (gov)
- CERTS (CERTS)
- Transit ISP (isp)
- TLD organizations (tld)
- NOGs & RIRs (nog)
- Registrants (rstran)
- Registrars (rsrar)
- Lobby / Policy (Lobby)
- Schools and universities (univ)
- Local communities (LC)

4.3. Combating Malicious Use

The Combating Malicious Use breakout session sought to foster consideration of vulnerabilities among various stakeholders, aid in cooperation, discussion and mitigation, enumerate attack surface, outline business continuity plan mitigations, perform gap analysis, and identify action items and stakeholders. The discussion broke the problem down into five core areas 1 – Registrants, Registrars, and Registries, 2) TLDs and the root, 3) Infrastructure, 4) Consumers, and 5) Cross-Boundary Issues, as depicted by the following graphic:



4.3.1. Discussion Summary & Recommendations

Registrants, Registrars, and Registries

Registrars (among others) populate the DNS, but no registrant verification means no source of trust; mechanisms are not in place to provide verification. Registrars are concerned with accreditation, reputation, and maintenance. Resellers and web hosting providers must have acceptable use or default policies. Registrars have commoditized High Value Domains (HVDs), offering different prices, features and security, but are still subject to transfers and hijacks and rarely offer multi-factor authentication or out of band communication (i.e. fax, physical) for changes. Some registrars can suspend domains or force "renew-only" for owners of domain being used maliciously. There are cases where registrars are merely proxies for resellers, and this poses concerns about security and abuse as well. This leads to the question of inter-registrar hijacking domains and processes for reclaiming those domains.

Registrants need awareness, are subject to social engineering (i.e. spear phishing with spoof of registrar queries as evidenced in the CheckFree incident in 2008) and registrant account compromise, and should require multi-factor authentication for changes to HVDs from their registrar. Domain names are assets, but owners rarely understand the value.

Registries haven't penetration tested EPP (Extensible Provisioning Protocol) and are at significant risk of flux churn enabling malicious use of the DNS. This leads to a debate over a domain owner's privacy versus accountability for malicious use. The WHOIS database inherently suffers from integrity issues, and no clear dispute resolution policy exists. For blacklisting registrations, who is involved or where should it be done, at the registry, registrar, resolver, or client levels?

Participants discussed how the DNS community can provide assistance in this area and ICANN's potential role with building alert lists, enabling cooperation as opposed to collusion, and vetting policy. The ICANN community collaboration process is viewed to need assistance – was any TACTICAL action taken in response to key events such as Srizbi or Conficker? There are collaboration opportunities between ICANN, registries, registrars, registrants, law enforcement, industry and security researchers to enable tactical responses via abuse and compliance teams. Note: The collaboration between these parties in response to the Conficker was publicly announced one week after the Symposium and represents the first step in collaborative tactical response.

Law enforcement needs better access to more optimized data in order to fight malicious activity, including integrity within WHOIS data, and validated registrant and registrar points of contact.

An example of domain hijacking was used to illustrate these issues. There is currently no way to pull back a domain once it's been transferred to another registry by the hijacker. The use of stronger authentication mechanisms for changes to important domain names should be made a priority as the risk stems from interaction between registrants and registries. Further, registries can turn to ICANN for assistance, but have limited latitude in these cases. Not all registries/registrars are using EPP and not every registrar follows ICANN. In any case, solutions to this issue must be scalable. A high value domain model was proposed in which the registrant interacts directly with the registry (bypass the registrar) and can "lock" the domain, in which case, registrars cannot make changes to the domain until it has been "unlocked" with the registry. This is available from some registrars as a premium service. Another model, based on DNS registrations as commodities was proposed – in that registrants should be able to pay more money for more security or protection. Domains are viewed as assets in some instances, while in others, the lowest possible initial investment is highly valued – there is a broad spectrum of users and most do not understand the risks associated with losing a domain name. Generically, more robust services or methods of ensuring accountability and quick response are needed, from EPP, to multi-factor authentication (fax, physical, etc), to protocol, to awareness.

It was proposed that security researchers should have access to special services to explore security problems (e.g. response to Conficker domain registrations). Presumably, if reverse engineered, security experts could block the seemingly random domains in advance, but procedures need to be established for this to occur. A forum to communicate with the security community is sorely needed – but the problem seems to be the mix of actors: ICANN, registrars, resellers, etc, and some of them are malicious actors in and of themselves. DNS Black Listing (DNSBL), and the registrar alert list are methods that are already in place, but one idea proposed was to block domain registration at the registry level. . However, the measures themselves may pose denial of services vectors and consideration should be weighed heavily as such.

TLDs & the Root

With regard to the root, root zone AXFR security, renumbering plans, RFC2870 update, route hijack protection, transparency of root operations, and use of monitoring data were mentioned as areas of concern. An understanding of what occurred to L root in Feb of 2007 was suggested as a method of examining the issues with root server operations. It was suggested that "golden networks" and Anycasting with better load distribution, at the cost of making detection more complex, would offer only some protection against route hijacking.

Concerns with gTLDs involved participation in publication of an "effective TLD list", and single label TLDs with implementation issues and having content at the apex. Further, general scalability concerns were raised with respect to IDNs, DNSSEC, IPv6 and new gTLDs. For ccTLDs, concern was expressed over lack of documented ccTLD policies and stability of registry organizations.

An incident response model is desired, with out of band responder and ISP access. Such a model would require creation and maintenance of a list of global players and response teams that are available for response. Further, procedures and exercising of those procedures would be necessary.

Various solutions at this level were instituting lame delegation checks, publishing a list of root server nodes and route origination locations to enable wider monitoring, and emergency TLD delegation changes. Suggested recipients of this information included upstream ISP, Internet Exchange Points, and new turn-ups to allow monitoring outside of the rootops community. Emergency TLD delegation changes could be used to cope with DDoS where a registry can redirect itself until the attack is mitigated.

Additional problems discussed included plans for new IDN TLDs conflicting with content in country-specific alternate roots and signed roots leading to an increase in alternate roots (a number already exist) by countries which refuse to participate in a single IANA root. Additionally, concerns were expressed over double flux attacks and the ability to detect them and discriminate between legit and malicious traffic.

Infrastructure

Infrastructure focused on authoritative servers, resolvers / recursive servers, ISPs, and generically, the transit network. In general, the DNS is viewed to make too many assumptions on the IP infrastructure it rides over. Further, when the DNS is attacked, the infrastructure suffers well beyond just the DNS.

For resolvers and recursive servers, concerns stemmed from cache poisoning and the passing of queries to the root that really shouldn't be passed. For the latter, authoritative servers generally have upward recursion issues, as there is no way in the specification to say "I Don't Know". De facto modification of the protocol has been to "query the root", and although helpful, implementations can be abused and the architectural impact of these implementations needs to be considered. It was suggested that stub resolvers address the generation of these queries. Many felt the paper by Peter Danzig provides a good background for understanding the issue. Additionally, physical attacks or access to the servers themselves, and the establishment of rogue resolvers (e.g. DNSchanger Trojan) were iterated as concerns. It was suggested that fuzzing (http://www.owasp.org/index.php/Fuzzing) and resolver testing, establishing a testbed, and detection of out of bounds / malformed queries be researched, and that renumbering guidelines be made available for recursive servers.

Regarding ISPs, two main issues were raised, 1) incident response and 2) DNS resolution services provided by the ISP. For incident response, route filtering data was generally noted as poor, and there is a lack of monitoring root / TLD prefixes. Most ISPs have response teams, but DNS is not expressly in their purview. The result is a need to link ISP response efforts to those within the DNS. Further, questions were raised on liability over poisoned caches, especially given that most consumers rely on their ISP for resolution. For ISPs that run local copies of root servers, if that copy becomes stale, do they inform their downstream users of a fractured root? Subscribers need to understand their reliance on the DNS

resolution services provided by their ISP, and if it's a critical need, they should consider having alternate resolution paths that will not be filtered or redirected in some manner by their network providers.

For the network generically, in protocol attacks, queries can be generated that use lots of resources and bogs down authoritative servers. The query response language is unbalanced and reflective attacks exploit this. With BCP #38, a collection of Best Community Practices related to network filtering as mitigation against DDoS attacks, DNS behavior is predicated on there being no network layer spoofing. With DNS response modification / synthesis, modification of DNS answers are being done in transit, specifically, NXDOMAIN rewriting with little concern over what it breaks downstream. There are also security issues related to this functionality (e.g. 2nd order effects of Kaminsky poisoning). With IPv6, there are scalability issues for session rates and DNS synthesis (A <> AAAA) not being signed by an authority.

Firewall rules were discussed as port 53 is used in many attacks as it is allowed through most firewalls. UDP packet length limits were noted to disrupt DNSSEC / EDNS eventually. There is no clear cut best practice and many tradeoffs exist.

Information sharing was once again identified as a concern, but in the context of distinguishing it from incident response. Data sharing (e.g. from DNS-OARC) is currently being done, but should also include data on bad actors and malicious traffic. As an example, .IN attacks are very difficult to detect because of a low query rate per "agent", and the fact that responses vary (e.g. SERVFAIL, refused, temporal stop, complete stop). Persistent errors are necessary, but require an understanding of which responses make a client try again opposed to fail hard and give up.

The concern over ENUM data was discussed – E.164.arpa is not used specifically because of privacy concerns. However E.911 and other emergency services have requirements that are or can be met via this data. Enumeration is trivial, and the recommendation was made to use private ENUM which has enclosures.

The "last mile" of DNSSEC (that between the consumer and a recursive resolver) was also discussed. The issue is that when a query request is issued, a signed answer is returned. In order to validate the response, additional queries must be sent directly to other authoritative servers and stub resolvers need full implementation to support this. A trusted path from stub to recursive server is required; otherwise full validation is required at the stub. To complicate matters, there is no visibility into failures.

Consumers

The target space grows as one moves down the line from ISP to consumer. Education at the end user level is seen to be critical and a consumer's edge protection devices are of concern. It was suggested that ISP security recommendations be used as a model for consumer education; based on BCP #38. A competing view was expressed as the expectation that little can be done at the consumer level and it should be as transparent as possible.

Edge protection devices such as broadband routers, firewalls, and set top boxes, the primary concern stems from integration of recursive resolvers. These boxes do not auto-update firmware, may interfere with DNS functions, or may outright manipulate DNS functions. Such interference and/or manipulation affects EDNS, DNSSEC and IPv6 implementations, and most devices have a 5-10 year life with no method of easily updating their functions. NAT devices suffer from a lack of port randomization, and hinder anomaly detection. All these devices

suffer from weak user awareness on the importance of security, and it was suggested that ISPs and vendors walk subscribers through the steps of setting up secure configuration (e.g. assigning passwords). It was also suggested that vendors might consider recall / update / coupon models for devices with issues or in lieu of that, an "End of Life" program for older devices.

Consumers rely heavily on DNS for operating system, application and mobile uses. Application auto-update programs need to consider implementing security instead of blindly trusting responses from the DNS. Operating system vendors might consider adding easy to interpret logs of DNS queries/answers to allow consumers to see who did what and when.

Cross-Boundary Issues

This area was not discussed due to time constraints, but key portions of it (e.g. law enforcement) were discussed throughout the other areas.

4.3.2. Open Questions

The following questions were brought up during the discussion and were unable to be answered or required additional research. They are mentioned here to preserve for and focus future efforts.

- In cases where registrars are just "proxies" for resellers, what are the security / abuse concerns?
- Are there cases of inter-registrar hijacking of domains, and if so, what protocols / procedures exist for reclaiming those domains?
- What is the Registry Internet Safety Group, what do they do and how can they be leveraged to support efforts against malicious use?
- Can the best practices regarding domain name registrations and blocking of malicious registrations be documented?
- Are there scaling issues with respect to DNSSEC, IPv6, gTLDs, and IDNs on the root and registries?
- In double flux attacks, what methods will enable detection and discrimination of legitimate versus malicious traffic?
- How should authoritative servers process queries they cannot answer? Can (and should) stub resolvers or recursive servers resolve junk queries (e.g. "localhost") at the root? In either case, what actions can be taken, and by whom?
- Should DNS servers be allowed to "fail to respond" to queries if they are convinced it is malicious?
- How can real time information be made available to the community; what regulations and constraints exist; and what compliance models will be violated?
- Are security related funding surcharges possible (e.g. from domains, from root use, other sources)?
- What is ICANN's role in enabling and helping inform and measure risk, setting strategic cyber priorities for the DNS, response, collaboration to improve accountability, combating malicious use, facilitating exercise collaboration?

4.3.3. Solutions and Possible Actors

The following actions and possible actors were particularly highlighted during the discussion.

- Establish more secure DNS registration models (e.g. lock, or pay for added protection), and include interaction with ICANN given registry agreements it has in place.
- Establish procedures for registering domain names on behalf of security experts to thwart malicious use of those names.
- Create an incident response model, to include CERTS and ISP and other roles along with incident response procedures (domain registration blocking among others); develop exercise program to test those procedures.
- Publish a list of root server nodes and route origin location information for increased monitoring beyond rootops.
- Create procedures for emergency TLD delegation changes to reduce impact of DoS attacks on a given TLD.
- Establish a common testbed and fuzzing capability for researchers to conduct out-of-bounds / malformed query testing.
- Use INOC DBA to provide a level of authentication for point of contact (POC) information, maintain a common POC location, and have it documented in NIAC vulnerability disclosure framework.
- Conduct awareness training (perhaps based on ISP security recommendations, BCP 38) and provide secure configuration assistance for consumers with edge protection devices from vendors and ISPs.
- Foster discussions between firewall and edge device vendors and DNS security experts. The DNS security experts generally would like devices to just pass DNS traffic and leave DNS security to the client and server, elements that can and are updated regularly. A coordination forum for consumer edge devices is needed and existing forums are viewed as insufficient.
- Modification of ISP acceptable use policies to account for malicious use.
- Information sharing mechanisms to exchange ideas and information on incidents and lessons learned in real time. Counter-incentives (e.g. privacy concerns) far exceed the incentives. It was suggested that the financial industry's information sharing model could be used as a basis for these efforts.

4.4. Combined Session

The combined session resulted from the merging of the Enterprise Use and Combating Malicious Use breakout sessions. Many overlaps between the two sessions were seen and it was believed that merging the two sessions would result in a more productive discussion.

4.4.1. Discussion Summary & Recommendations

As a combined session, an attempt was made to compile a list of the big questions for research – if the operations-minded people could create the questions, researchers could solicit grants and develop solutions. See the open question section for this list.

Generally, the view was that combating malicious use need to be approached strategically instead of reactively as is occurring now. The law enforcement community requested experts to collaborate with them on cyber crime issues and needs open source / low cost tools to do it. International cooperation, best practices and other high level approaches need to be examined to determine what can be done within that realm. Most participants agreed that ICANN needs to establish the agenda and document the outcomes of DNS stakeholder meetings; previous meetings have gone without follow-up. ICANN is also working to improve the WHOIS data resolutions process via authenticated bulk submissions, but the suggestion was made to have operators periodically test WHOIS data for accuracy; while some efforts to accomplish efficiently exist, they need to be documented and shared with the community.

A presentation was made by Rod Rasmussen on the CheckFree domain hijack that occurred in the last quarter of 2008 which exemplified many of the issues discussed during the session. CheckFree.com is considered a high value domain, and a lot of implications stemmed from this attack as bill pay services were shut down for day. The attackers were able to steal the registrant's username and password used to make changes to the authoritative DNS servers for the domain – this was an attack on the registrant, not the registrar and highlights the problems with single-stage password only authentication methods. Other financial institutions that relied on CheckFree (e.g. NAME.checkfree.com) were also affected by this. While CheckFree took control of the domain within 8 hours, the TTL (set to 48 hours by the attackers on purpose) resulted in a much larger window of exploitation. This case highlighted several interesting issues:

- Recommended upper TTL limits
- Are there best practices for operating a cache – do operators understand the tradeoffs and risks associated with caching?
- With regard to incident response, how can owners collaborate with providers for solving the problems faster (e.g. flushing caches prior to expiration)? Are there technical solutions (e.g. signal a cache flush via the protocol)?
- Are there tools or processes which can increase a domain owner's situational awareness and detect these attacks?

4.4.2. Open Questions

- Query Pollution – what is it, how can it be mitigated?
- How can DDoS against DNS be mitigated? Is an out-of-band control system feasible as a solution?
- How can users and / or ISPs detect traffic "damage" on the Internet? What would enable ISPs to conduct more analysis on their network's traffic?
- How much of BCP #38 (methods of filtering against DoS attacks) do ISPs need to adopt to achieve a percentage reduction in DDoS effects?
- Can a model be developed to see what happens if applications chose to ignore the DNS? (e.g. Microsoft's P2P DNS)
- Can procedures which cross international boundaries be establishing for detecting (technical) and prosecuting (political) cyber criminals?
- What impacts does Google's Chrome pre-caching have on the DNS?

- Is there a good architecture for putting organization boundaries in DNS?

4.4.3. Solutions and Possible Actors

The following actions and possible actors were particularly highlighted during the discussion.

- Future DNS stakeholder meetings with set agenda and documented follow-up actions.
- Examine international cooperation, best practices and other strategic approaches to combat malicious use.
- Establish collaboration between law enforcement and security communities, enabling communication and technical assistance in investigations.

5. Next Steps

The Symposium resulted in a slew of questions regarding DNS risk factors and recommendations to address mitigation, but few actors were identified. The first priority should be to establish a collaborative process to set priorities, goals, select task leads, initiate work and measure progress of the projects and questions selected for implementation. Based on the common themes and actionable solutions proposed in the breakout sessions, a few solutions establish themselves as ideal candidates for further study:

- Research into a DNS collaborative incident response function to provide information sharing and coordinate incident response actions within the community.
- Creating and delivering awareness education to all stakeholders and determining appropriate mediums for reaching those groups. Education should include spectrum from general awareness to advanced training, and cover both technical and non-technical topics.
- Establish a roadmap to carry on the work conducted at this Symposium and encourage continuing, cross-functional dialog among a wide range of DNS stakeholders.

6. Conclusion

The Symposium discussions resulted in identification of the central issues, current efforts, and possible solutions to issues facing the DNS and validated the need and benefits of ongoing collaboration across fields. The Symposium merely scratched the surface of what needs to be done with respect to security, stability and resiliency of the DNS. As evidenced by the long lists of open questions, there remains significant opportunity for additional study and collaborative efforts.

Appendix A: Attendance Roster

Last	First	Last	First	Last	First
Ahamad	Mustaque	Koch	Peter	Torres	Oscar
Akkerhuis	Jaap	Kolkman	Olaf	Twomey	Paul
Allor	Peter	Krasser	Sven	Ulevitch	David
Alperovitch	Dmitri	Kristoff	John	Vaughn	Randy
Antonakakis	Manos	Lanstein	Alex	Vergara	Mauricio
Arends	Roy	Larson	Matt	Vicente	Carlos
Black	Nick	Lawrence	David	Vixie	Paul
Bonis	Pierre	Lemon	Ted	Watson	Carlos
Bortzmeyer	Stephane	Lewis	Ed	Weiler	Samuel
Burkov	Dmitry	London	Jacqueline	Wessels	Duane
Claffy	K	Matsuzaki	Yoshinobu	Wilhoite	Wally
Collins	Michael	Mauch	Jared	Woolf	Suzanne
Crain	John	Maughan	Doug	Wouters	Paul
Crocker	Steve	McPherson	Danny	Zimmerman	Ralf
Cross	Thomas	Miorelli	Bob		
Dagon	Dave	Mohan	Ram		
Daly	Tom	Montgomery	Doug		
Davies	Kim	Mwangi	Michuki		
Dougherty	Chad	Ogielski	Andy		
Duncan	Jim	O'Reirdan	Michael		
Durand	Alain	Perrin	Brandon		
Edmonds	Robert	Piscitello	Dave		
Eland	Howard	Pounsett	Matthew		
Evans	Chris	Purdy	Andy		
Filip	Ondrej	Rasmussen	Rod		
Fomenkov	Marina	Rattray	Greg		
Goodman	Sy	Regan	Michael		
Grasso	Tom	Ritchie	Norm		
Griffiths	Chris	Robachevsky	Andrei		
Hall	Martin	Roosenraad	Chris		
Harris	Vernita	Rose	Scott		
Heifa	Sergius	Schmidt	Jeff		
Henry	Max Larson	Schnizlein	John		
Irwin	Tim	Shannon	Colleen		
Ito	Yurie	Sima	Caleb		
Joffe	Rodney	Sood	Arun		
Kaiser	Michael	Sury	Ondrej		
Kaminsky	Dan	Thompson	Mary Claire		
Kane	Paul	Thorne	Nick		

Appendix B: List of Framing Presentations and Supporting Material

- **Crain, John - ICANN**
  "DNS It's Not Just the Protocol"
  Presentation: http://gtisc.gatech.edu/pdf/Crain_DNS_Symposium_2009.pdf
  Supporting Material: http://gtisc.gatech.edu/pdf/DNSSSRPaper.pdf

  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.

- **Dagon, David - GTISC**
  "DNS Attacks and the Projection of State Power on the Internet"

  Malicious overlay networks (e.g., botnets) have matured into an instrument of state cyber power. State actors now see DNS attacks as a form of political expression, a means of projecting power onto the Internet, and as a vehicle for amplifying geopolitical disputes. Recent conflicts have demonstrated the utility of surgical DNS poisoning, in addition to traditional DDoS attacks. This new era will provide deeper challenges to the resilience of Internet protocols, and complicate the development of Internet governance.

- **Kaminsky, Dan - IOActive**
  "DNS: What Do You Mean, It's At The Heart Of The Internet's Security Model?"

  DNS is insecure and unauthenticated. The Internet is built on DNS, as it's the only thing that federates across organizational boundaries. Therefore, the Internet is insecure and unauthenticated? Apparently, even surprisingly so. I will talk about concrete attacks that in a perfect world, would never have been possible. But it's not a perfect world, and DNS is far more important than even I expected. DNSSEC is needed after all.

- **Kolkman, Olaf - NLNetLabs**
  "A Perspective on Categorizing Problems"
  Supporting Material: http://www.nlnetlabs.nl/downloads/publications/se-consult.pdf

  When dealing with Security and Stability issues related to DNS it is important to identify the ultimate source of the issues and understand which actors may be involved in solving them. One perspective is provided that may be of assistance when trying to categorize or understand issues.

- **Rose, Scott – NIST**
  "The Challenges of Managing Secure DNS in the US Federal Government"

  Deploying and managing DNS within the US Federal Government presents a different set of challenges than just a single enterprise. The .gov domain is made up a heterogeneous mix of organizations and networks. Some of which have overriding security mandates and policies that influence how DNS is to be set up and managed. This is especially true with the deployment of DNSSEC within the .gov TLD.

Appendix C: Symposium Agenda

Christopher Klaus Advanced Computing Building, GTISC, Atlanta, Georgia, USA

February 2, 2009

1700 – 1730	Pre-Registration	Klaus Atrium
1730 – 1930	Welcome Reception	Klaus Atrium

February 3, 2009 – Day 1

0730 – 0800	Registration	Klaus Atrium
0800 – 0815	Logistical Notes *John Crain*	Klaus 1116
0815 – 0830	Welcome & Symposium Opening *Dr. Mustaque Ahamad (GTISC) & Dr. Greg Rattray (ICANN)*	Klaus 1116
0830 – 0835	Introductions *Dave Dagon & John Crain*	Klaus 1116
0835 – 1000	Framing Presentations and Panel *Chair: Paul Vixie, Presenters: John Crain, Dave Dagon, Dan Kaminsky, Olaf Kolkman, Scott Rose*	Klaus 1116
1000 – 1015	Morning Break	Klaus Atrium
1015 – 1100	Breakout Session Overview & Expectations *Organizer: John Crain, Session Chairs: Danny McPherson, Michuki Mwangi, Chris Roosenraad*	Klaus 1116
1100 – 1130	Assignment of Groups *Session Chairs: Danny McPherson, Michuki Mwangi, Chris Roosenraad*	Klaus 1116
1130 – 1230	Lunch	Klaus Atrium
1230 – 1630	Breakout Sessions	Varies
[1445 – 1500]	Afternoon Break	Klaus Atrium
	DNS and the Enterprise *Session Chair: Chris Roosenraad*	Klaus 1116 East
	DNS in Resource-Constrained Environments *Session Lead: Michuki Mwangi*	Klaus 1212
	Combating Malicious Use of the DNS *Session Lead: Danny McPherson*	Klaus 1116 West
1630 – 1700	End of Day Wrap-Up *Dave Dagon & John Crain*	Klaus 1116
1730 – 1830	"Meet the GTISC Students" Open Discussion *Informal discussion with GTISC students – open to all attendees*	Klaus Atrium

February 4, 2009 – Day 2

0800 – 0830	Welcome Back, Opening Remarks, & Expectations *Dave Dagon & John Crain*	Klaus 1116
0830 – 0930	Preliminary Review of Breakout Sessions *Session Chairs: Danny McPherson, Michuki Mwangi, Chris Roosenraad*	Klaus 1116
0930 – 0945	Morning Break	Klaus Atrium
0945 – 1500	Breakout Sessions	Varies
1130 – 1230	Lunch	Klaus Atrium
	DNS and the Enterprise *Session Lead: Chris Roosenraad*	Klaus 1116 East
	DNS in Resource-Constrained Environments *Session Lead: Michuki Mwangi*	Klaus 1212
	Combating Malicious Use of the DNS *Session Lead: Danny McPherson*	Klaus 1116 West
1500 – 1515	Afternoon Break	Klaus Atrium
1515 – 1615	Breakout Session Presentations *Session Leads: Danny McPherson, Michuki Mwangi, Chris Roosenraad*	Klaus 1116
1615 – 1700	End of Symposium Wrap-up, Critique, & Next Steps *Dave Dagon & John Crain*	Klaus 1116
1700 – 1715	Closing Remarks *Dr. Mustaque Ahamad (GTISC) & Dr. Greg Rattray (ICANN)*	Klaus 1116

Appendix D: Enterprise Use Breakout Session Guide Book

- Understanding enterprise DNS reliance and enabling effective risk mitigation -

Session Chair: **Chris Roosenraad - chris.roosenraad@twcable.com**

Description:

Large enterprises have a number of internal operational and external market-facing dependencies on the DNS. Failures including the presence of inaccurate data in the DNS or the lack of availability of DNS functionality could impact business significantly to include lost revenue, increased expenses, negative impact to reputation, and exposure to liability.

Enterprises typically utilize various risk management techniques to manage business and technical risks. With respect to DNS risks, most enterprises do not have sufficient visibility into DNS dependencies nor do they have the supporting data to perform a thorough risk analysis.

Tasks:

(Specific actions which should be accomplished over the course of the Symposium)

- Gap Analysis of Central Issues (what's missing from this list?)
- For each issue, what is the current approach to solving them and who is involved in them?
- For each issue, what needs to be done, and who _should_ be involved in the solution?
- Do the needs and current approaches match?
- For each issue, establish a roadmap of prioritized, actionable items defining who/what/when

Focus Areas:

- Are there specific case studies, examples, or anecdotes which can be used to focus the discussion?
    - Bank of America, Level3, SunTrust, IBM, HP, UTC?

Central Issues:

(Issues to frame and focus the discussion of solutions and a mitigation strategy)

- Level of awareness of enterprise reliance on DNS for critical services
    - Do they understand their reliance on the DNS and to what extent?
    - Do enterprise's currently do risk management with respect to their use of the DNS?
        - Are they making any assumptions?
    - What do enterprises currently do for monitoring external infrastructure they rely on?
        - Continuous monitoring of high-value domains from various points (ala DNSMon)
    - Are there training and awareness programs that any enterprise can utilize?
        - Would a "DNS For Dummies" type book help?
        - Trade shows, conferences, business continuity venues?
- How are an enterprise, its employees, and its customers affected by the DNS?
    - Cache Poisoning?
    - Domain hijacking
    - Phishing?
    - What are the solutions / costs / alternatives?
    - Are there collaborative, policy, governmental methods of helping enterprises better manage DNS risks?

Attendee Comments:

- What are the obstacles to deployment of DNSSEC?
  For example, use of "views" in BIND-9 complicates the signing of internal and external versions of an organization's zone, to say nothing of trust anchors.
- Is your caching infrastructure ready for DNSSEC?
- Do your internal tools/apps use DNSSEC?
- Are you ready for v6? AAAA?
- Are your internal tools/apps ready for v6 & AAAA?
- Do you need to support customers who are running DNSSEC and/or v6?
- When do you require everyone to be DNSSEC and/or v6 ready?
- What are the issues of bootstrapping trust (both in a DNSSEC and non-DNSSEC world) in DNS for mobile systems and public networks?

Appendix E: Resource Constrained Environments Breakout Session Guide Book

- Meeting challenges to secure & resilient DNS operations in resource constrained environments -

Session Chair: **Michuki Mwangi – mwangi@isoc.org**

Description:
DNS operations pose unique challenges in environments where limited bandwidth, high latencies, unreliable equipment environments, and limited budgets are the norm. In many cases, the focus is on efficient operations; while sophisticated risk management may not be feasible, a systemic approach to identifying and managing a limited set of risks is desirable

Tasks:
(Specific actions which should be accomplished over the course of the Symposium)

- Gap Analysis of Central Issues (what's missing from this list?)
- For each issue, what is the current approach to solving them and who is involved in them?
- For each issue, what needs to be done, and who _should_ be involved in the solution?
- Do the needs and current approaches match?
- For each issue, establish a roadmap of prioritized, actionable items defining who/what/when

Focus Areas:

- Are there specific case studies, examples, or anecdotes which can be used to focus the discussion?

Central Issues:
(Issues to frame and focus the discussion of solutions and a mitigation strategy)

- Bandwidth / Service Availability
    - Are there provisioning solutions that are tailored to this environment?
    - Are there governments or organizations that can subsidize operators in this environment?
    - Do operator contingency plans exist? Have they been tested?
    - What are the threats to bandwidth & service availability?
    - Are there political or policy issues which impact bandwidth and availability?
    - Are there better tools / implementations that can increase bandwidth & availability?
    - Are there collaborative efforts (and by who) that can help?

- Trained Operators
    - What are the gaps in operator knowledge?
    - Where do operators currently get their training?
    - Are there current training solutions?
    - ICANN, ISOC, & NSRC awareness and technical training programs
    - Are they adequate?
    - Are the operators trained in security & incident response?
    - Will a DNS/CERT function help the community?
    - Is there a better way to increase number / quality of trained operators?
    - Common resource for DNS information (book, website, recurring conference, etc)

        - Technical training (NOG, education systems)

- General Awareness of the DNS Across Organizations
    - What is the current thought on level of DNS awareness
    - What are the methods of increasing DNS awareness?

- Outsourcing
    - Are outsourcing options available?
    - Do operators understand the operational and security implications of outsourcing?

Attendee Comments:

- Resource Constrained Environments is not only for remote outposts in Africa. It is also the case of many organizations in richer countries, which have no knowledgeable human resources available and still must operate their DNS securely.
- My experience with DNS configuration support (for instance in the ".00" registry which mandates thorough technical tests when delegating a domain) is that current DNS knowledge is already too low in most organizations, not to mention DNSSEC!
- What would be the better practice to try to secure a DNS operation in this environment?
- Collaborative Anycast Network among ccTLDs and/or network operators
- Best practice and comments on using Bind secure template (cymru)
- Automatic update of the bogon ACL (techniques, tools, project)
- Monitoring
- How to deal with DDoS Attack
- OS Software, Software choice

Appendix F: Combating Malicious Use Breakout Session Guide Book

- Identifying and improving collaboration in combating malicious activity leveraging the DNS –

Session Chair: **Danny McPherson – danny@arbor.net**

Description:

The DNS is used in unintended ways to facilitate or magnify malicious acts. Many of these uses are not contrary to technical specifications, but rather in violation of contract, law, and/or industry accepted norms and best practices. As such, a comprehensive approach to addressing this class of risks is required.

Tasks:

(Specific actions which should be accomplished over the course of the Symposium)

- Gap Analysis of Central Issues (what's missing from this list?)
- For each issue, what is the current approach to solving them and who is involved in them?
- For each issue, what needs to be done, and who _should_ be involved in the solution?
- For each issue, what are the gaps between what needs to be done and the current approaches?
- For each issue, establish a roadmap of prioritized, actionable items defining who/what/when

Focus Areas:

- Are there specific case studies, examples, or anecdotes which can be used to focus the discussion?
    - Srizbi BotNet?

Central Issues:

(Issues to frame and focus the discussion of solutions and a mitigation strategy)

- Definition of Malicious Traffic
    - Are there organizations / governments attempting to define this?
    - Are there common baselines?
        - Are there classes of malicious traffic (i.e. clearly bad, maybe bad, not so bad)?
        - Typo squatting, front running, tasting
        - Bots & BotNets
        - Use of DNS for reflection attacks
        - DDoS
        - Route Hijacks
        - Zone Integrity
        - Cache Poisoning
        - DHCP Malware, Rogue DNS
        - Open Resolvers
        - Spam / Phishing
        - Fast Flux
        - Enumeration / Reconnaissance
    - Is a global approach possible?
    - What organizations are best suited to define this?
- Actors within The Malicious Traffic Space
    - Who are the Good Actors
    - Who are the Bad Actors

        - Malicious or Compromised Registrants / Registrars / Resellers
        - Abnormal amounts of malicious traffic
    - Who are the Victims?
- Detection of Malicious Traffic
    - Who is best suited to detect malicious traffic?
    - What are the current detection strategies and are they sufficient?
        - Are covert channels detectable?
    - Are there established best practices for detection?
        - Is there a central clearinghouse for detection strategies?
        - Does a DNS CERT function make sense?
    - Have / Are Kaminsky-style attacks occurring? Why hasn't it been widely discussed?
- Response to Malicious Traffic
    - Is, or should, the detection and response be done by the same organization?
    - Are organizations who do detection even able to respond?
    - Do the victims of attacks perform response or do they "outsource" or ignore?
    - What would facilitate detection and response from different organizations?
        - Agreements, Policy?
    - What happens when malicious traffic crosses international jurisdictions, and/or when multiple nations or organizations are involved?
        - How does international law affect response?
        - Do agreements exist to facilitate multi-national response to malicious traffic, and if not, can they be reached, and by who?
    - Where do governments, law enforcement, and internet policy makers fit in this?
- Are there ways to preclude or proactively reduce malicious traffic?
    - Hosting agreements & Usage Policies?
    - Malicious Registrants?
    - Takedown procedures?
    - Community De-peering?
    - Do best practices exist in this area and is there a central clearinghouse to publicize them?
    - Research & Technical approaches?
    - Collaborative approaches?
    - Route Monitoring
    - BCPs for Registrars, registries, rootops
- Other Issues
    - What makes the DNS so attractive a medium for malicious use?
    - DNS Synthesis?
    - ccTLD vs. gTLD & Considerations
    - Emerging Topics: IPv6, DNSSEC, IDNs
    - High value Domains

Attendee Comments:

- Perhaps it goes without saying, but I'd like to hear some discussion about the use of DNS as covert channels in the course of attacks.
- An issue for consideration, proactive notification to administrative contacts of systems identified with weaknesses.

- An issue for consideration, the confusion being caused by increasing use of name registrations or local name resolution redirection for "bad" names.
- A thought for consideration, lack of site-local security-oriented knobs and features in the de-facto implementation, ISC BIND (e.g. no regex based name resolution control). Potentially lots of good this doing us (limits confusion and inconsistency), but does this put pressure on putting worse hacks elsewhere?
- A question for consideration, why wasn't there the poisoning problem some thought we'd see after the Kaminsky disclosure?
- A question for consideration, what are the practical limitations for ICANN policy to enforce and encourage better registrar cooperation and overall DNS security and stability from all players? What are the bottlenecks and ratholes?
- A question for consideration, when is it time to revisit developing a new or alternative stub resolver code base? There is potentially a lot of "useful" things to do at the edge client to help improve security.
- A few topics I would like to be brought up is the potential revocation of purely malicious domain names, potential reassignment of such names to researchers, and possibly forcing registrars to give up the payment information for those who purchase such names.

Appendix G: Symposium Feedback Trends

An online survey containing eight questions about the symposium was made available to all attendees for one week following the end of the Symposium. Of the 92 confirmed attendees, 32 responded. The following highlights the major trends noted in the responses.

Did you find the Symposium useful (why or why not)? Do you expect the outputs of the Symposium to be useful to the community?

Overall response was positive; primarily due to bringing stakeholders from across the DNS community together; some negative responses on lack of focus; sentiment that it remains to be seen whether outputs will be useful

Were the breakout sessions useful (why or why not)? Did you find the published guidebooks useful or constraining, and in what ways?? Do you have recommendations for breakout session topics?

General consensus was that the breakout sessions were useful, but some were disappointed that they could only attend one of the three; mixed reaction to the guide books; no suggestions for session topics were offered.

Was the Framing Panel useful?

Generally positive; helped in establishing sense of direction.

What part of the Symposium was most useful? Least useful?

Breakout sessions were most useful followed by networking opportunities; not having pre-set goals at the start of the breakout sessions was least useful.

Do you have suggestions for disseminating the output (information & recommendations) of the Symposium?

Publishing a white paper, edited discussions, and identification of common themes across sessions.

Would you attend future iterations of this Symposium?

27 Yes, 2 No, 3 No Answer

Do you have any suggestions for improving this Symposium?

More time; more focused sessions, defined goals, and broader representation of attendees.