

## **Global DNS Risk Symposium**

The ICANN/GTISC Global DNS Risk Symposium will bring together representatives from across DNS ecosystem stakeholder groups (technical development, network operators, enterprise users, and security experts) for the purpose of improving the security, stability and resiliency of the DNS.

The Symposium is designed to present, integrate, and expand on previous research and work, and will focus on the analysis of risks from three perspectives (large enterprise, resource constrained environment, and combating malicious use).

The Symposium seeks to define cross-functional approaches to produce actionable mitigation strategies to risks within the three focus areas. As a recurring event, future symposia will refine strategies produced at previous events, and collaborate on new ones.

### **Venue and Attendance**

3-4 February 2009, Georgia Tech Information Security Center (GTISC), Atlanta, Georgia, USA

Attendance is by invitation only

### **Symposium Chairs**

- John Crain (ICANN)
- Dave Dagon (GTISC)

### **Symposium Steering Committee**

The steering committee is comprised of members representing key areas of DNS operations, use of DNS in resource-constrained environments, use of DNS in large enterprises, malicious use of the DNS, technical implementations, and DNS standards.

- Alain Aina
- Olaf Kolkman
- Rod Rasmussen
- Yurie Ito
- Peter Koch

### **Specific Focus Areas**

- Understanding large enterprise DNS reliance and enabling effective risk mitigation
- Meeting challenges to secure & resilient DNS operations in resource constrained environments
- Identifying and improving collaboration in combating malicious activity leveraging the DNS

### **Outcomes**

- Baseline relevant research and create a communal understanding of current state of the DNS
- Identification of cross-functional stakeholders necessary to creating effective risk mitigation strategies for each of the focus areas
- Increase understanding of dependence on, risk associated with, and operational impact of disruption or corruption of the DNS may cause
- Identification and first-order evaluation of potential risk mitigation strategies appropriate to each of the focus areas
- Collaboration on a work plan which defines an actionable, cross-functional approach to implement a risk mitigation strategy for each focus area
- Determine format for recurring symposia and define measures of effectiveness for evaluating usefulness and impact of symposium efforts

## **Managing the risks of DNS in the large enterprise**

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. To address these voids, the Symposium seeks to:

- Understand the current level of DNS risk management occurring in enterprise environments;
- Understand the risk assumptions and parameters being used in enterprise DNS risk management;
- Understand the perceived and real costs of risk mitigation techniques;
- Identify tools, research, or other activities that would help enterprises better manage DNS risk,
- Identify collaborative efforts that will help fill the information voids.

## **Managing the risks of DNS in resource constrained environments**

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.

The Symposium seeks to:

- Understand current visibility into DNS risks in resource-constrained environments;
- Understand the desire and ability to manage classes of risks;
- Understand current mitigation options and strategies;
- Explore potential mitigation options suited for such environments;
- Explore opportunities for research, tool development, and collaboration to enable more effective DNS risk management in such environments.

### **Managing the risks of the DNS being leveraged in other malicious acts**

We have seen the DNS 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.

The Symposium seeks to:

- Understand classes of unintended DNS use;
- Understand mitigation strategies:
  - Technical standards
  - Technical mitigations and countermeasures
  - Technical and administrative tools
  - Technical and administrative policies, procedures, and best practices
- Discuss involvement and role of government, regulators, and law enforcement;
- Discuss the impact of international law and jurisdictional issues;
- Explore opportunities for research, tool development, and collaboration to enable more effective mitigation of DNS-leveraged attacks