OARC Briefing

DNS Operations, Analysis and Research Center

OARC Mission/Motivation

The DNS is one of the most visible and mission-critical pieces of infrastructure underlying today's Internet. When the DNS stops working, so do all other applications, not just in the part of the Internet directly affected but potentially globally. A stable, reliable and secure DNS is key to maintaining public and government confidence in the management of a functioning Internet, and supporting innovation and its expansion.

The Internet industry today collectively faces some severe challenges from those with criminal and extremist malicious intent. These miscreants are driving a plague of spamming, phishing, botnets, DDoS, malware, spyware and other abuse, which is causing significant harm and expense to Internet end-users, providers, and society in general.

The DNS system is currently heavily implicated in both perpetration and as a target of this abuse. Recent examples include the BotNet DDoS attack against the root servers on 6th February 2007, and the use of open recursive DNS resolvers to amplify an attack against various root and TLD operators in early 2006. "Pharming" vulnerabilities in end-user equipment have been identified which could allow wholesale hi-jacking of all DNS queries to fraudulent sites. None of these types of problems are unlikely to diminish in the short term.

OARC (http://public.oarci.net) exists to both co-ordinate and be part of the response to these challenges. During operational incidents, OARC enables rapid sharing of critical information with the key trusted contacts in affected organizations which is key to mitigating the impact. Post-incident, OARC's significant data capture and forensic analysis capabilities help track the cause and perpetrators. Additionally, OARC's outreach to the research, vendor and end-user communities develops the means to prevent such incidents in future.

History and Governance

OARC was founded by Internet Systems Consortium Inc. (ISC) in 2004, as part of a joint research proposal with CAIDA to the National Science Foundation. The NSF funding award was used to procure OARC hardware for data collection and analysis, and the OARC secretariat is operated on an ongoing basis by ISC. ISC is a nonprofit 501(c)(3) public benefit corporation which develops the leading *BIND* DNS server and other Internet-critical software, and operates the **F** Root Server instance.

OARC was conceived as a membership organization where DNS operators, network researchers, software implementors and others could participate to share data, common problems and solutions in a secure environment. Currently OARC has over 40 members, including 6 root server operators, over a dozen TLD operators, DNS product & service vendors, Regional Internet Registries, and researchers (see attached schedule for a full list of current members). This is growing at a rate of around 1 per month. All members are asked to sign the OARC Membership and Data Access Agreement, which places obligations on OARC and all members to respect the confidentiality of data gathered and shared.

At present OARC operates as a semi-autonomous program within ISC, and obtains slightly less than half its operating costs from membership subscriptions, the remainder as cross-subsidy from ISC. The longer term objective is that OARC should be capable of being fully autonomous from both a funding and governance point of view, operated by and for its members, and acting in a neutral fashion to all of them. The first steps towards this will be taken this summer, when elections for the OARC Policy Council are conducted.

Although it is less likely that OARC will pursue further major research program grants from public bodies such as the NSF, seeking further external funding from e.g. law enforcement, or for specific infrastructure/projects, is not ruled out in future.

Member Benefits and Services

Successful membership organizations provide quality tangible services of direct benefit to their members, and this is very much part of OARC's mission. Current services include:

- **A secure, encrypted, jabber-based chat server** to give a rapid means of reaching trusted contacts and enabling real-time multi-party discussions. For instance, this was used by root operators during the 6th February root server attack.
- **Public and Member-only mailing lists** for discussion of current DNS operations issues.
- **A private shared ticketing system** for reporting and auto-notification of DNS-impacting incidents.
- **Domain statistics collection** - using DSC software, OARC gathers summary data from root and TLD operators globally, and makes this available to members via a graphical interface. OARC also regularly takes part in the "Day in the Life of the Internet" data-gathering exercises where more detailed logs of all queries to participating servers are captured over a 48-hour period, and has the capability to turn this full logging on during incidents, as was enacted during the 6th Feb 2007 attack.
- **Large-scale server infrastructure** to upload, share, and analyze data with other OARC members - this is not confined just to DNS statistical and data capture, but can include vulnerabilities, malware, phishing data, blacklists and other imminent threat information.
- **Closed private mailing lists** for discussion of DNS operational security. Due to the often security- and business-sensitive nature of these discussion, participation in these is at the discretion of sponsoring OARC members only.
- **Twice yearly member meetings** at which DNS operations issues are presented and discussed. (For proceedings of the most recent meeting, see http://public.oarci.net/oarc/workshop-2006/agenda/)
- Ability to elect seats to the Policy Council which steers the direction of OARC.
- Interaction with key technical people at OARC's over 40 members, including root and TLD operators, DNS registries, DNS software implementors, researchers and law enforcement.

OARC's framework for information sharing and operational communication underpins all this - getting early warning of problems can limit operational impact for a business, keep customers happy, and save money. OARC's mission can be described as leveraging shared interests and contacts among its members as a "trusted introducer". Having technical personnel learn "inside information" from their peers that they might not otherwise meet, can be the most effective way of gaining timely new knowledge at a fraction of the cost of sending them on training courses.

OARC Public Benefit

OARC inherits ISC's central mission of public benefit, and provides a vehicle for its members to act not just in their own interest, but towards the greater good of the Internet community as well. This is particularly important as more reliance is placed on the DNS every year to support current and future Internet-based activities and applications.

A critical component of OARC's capabilities and contribution is the availability of raw operational data. Many of the detailed underlying principles of Internet traffic engineering and failure modes are in fact poorly understood, and the only way to improve this state of affairs is application of the scientific method to the study of these on the large scale. However, the network operators who are in the best position to gather measurement data are not best resourced to perform analysis of this data. While the research community has both the skills and will to do this analysis, they cannot always easily obtain suitable data.

Forensic data analysis is also of immense value to law enforcement in tracking the perpetrators of crimes and infrastructure attacks. There are however concerns about privacy of end-user data gathered from the network, as demonstrated by the recent incident where a large on-line service provider, motivated by the well-intentioned aim of making data available to researchers, carelessly placed raw data in the public domain and breached the privacy of their end-users with damaging consequences.

Making network data available to researchers and law enforcement, if done with appropriate safeguards, is clearly very much in the public interest, and OARC gives its members a way to demonstrate they are acting for the benefit of the community while minimizing risks to themselves.

It's also important to note that not all the threats to reliable, secure Internet operation are malicious. Studies performed by OARC partners such as CAIDA demonstrate that a significant amount of unwanted DNS traffic and operational problems are caused by misconfiguration of DNS or applications that depend on it. Part of OARC's mission is outreach to end-users, vendors and network operators to ensure that key knowledge reaches those who most need it.

The Internet industry has a long tradition of effective self-governance and self-regulation, and OARC seeks to continue this. Being seen, as an industry, to be responsibly and pro-actively tackling some of the most difficult issues facing us is not merely good business practice, but an effective strategy for heading off avoidable regulatory intervention.

OARC Future Evolution

OARC has been placed on a more stable footing, and undergone a review of its status and role since Keith Mitchell's appointment on 1st October 2006. It is clear that OARC performs a key role for which the membership growth indicates there is increasing demand. The challenge for taking OARC forward is not lack of opportunities, but rather identifying, resourcing and pursuing those where it can make the biggest difference.

The following development objectives have been identified for OARC over the next 6-18 months:

- Increasing the proportion of funding from member subscription sources to allow OARC to be fiscally self-sustaining and to grow staff numbers.
- Development of OARC's web site content and policy/procedure documentation.
- Fully autonomous governance structures in place.
- Development of OARC's trust model and collaboration tools to allow members to fully share information confidentially with self-defining sub-groups of other members, with equal ease in web, ticketing, e-mail, jabber, data gathering/storage, and other media as appropriate.
- Next generation data collection and storage infrastructure.
- Enhanced capabilities for distributed monitoring of root, TLD and ENUM servers.

Finally, it has been clear for some time that the OARC model could apply to Internet operations beyond the existing scope of DNS. There are many additional projects OARC has been approached to assist with, such as hosting malware and anti-phishing repositories, an Internet research on-line review journal, and acting as a safe-harbor for vulnerable anti-abuse resources, to name a few.

The success of OARC in growing and enabling its existing DNS-based activities would create the potential to expand into these and many other fields, making a significant positive difference to Internet operations generally.

OARC Subscription Levels

Category	Type	Annual Subscription	Contacts
1	Normal	$4200	3
2	Expanded	$6800	5
3	Beneficial	In-kind	
4	Supporting	$10000	8
5	Sustaining	$25000	12
6	Sponsoring	$50000	15
	Affiliate	Submit and Access Data	
	Associate	Access Data only	
	Contributor	Submit Data only	

Summary of Benefits of OARC Membership

- Direct real-time assistance and information from TLD and other root server operators in the event of another DDoS attack against members' infrastructure, to promptly mitigate impact and help with detection and prevention. OARC can help each member expand the resources available to them as it has for other root and TLD operators.
- Being able to demonstrate to customers, governments, law enforcement, media and the public members are supporting action to tackle serious network abuse issues such as BotNets that threaten Internet stability, reliability and security, without having to dedicate significant internal resource to this.
- The possibility of having an ongoing objective source of quantifiable data and peer-reviewed research knowledge to answer specific questions each member needs addressed.
- Ability to share data appropriately with the research community, contributing to the long-term public benefit of the Internet.
- Opportunity to track best operational practices at TLD and other root name servers to reduce costs and improve services towards achieving operational excellence.