

Ram Mohan comments on [Priorities for the long term stability of the Internet](#)

IGF, Vilnius [September 14, 2010]

Session 1: "What incident(s) would have the most negative impact on the Internet?"/ "What is the one thing that should not happen?"

As some of you may know, a big part of my day job involves the operation and management of top level domains at Afiliis. In total, we manage about 17 million domain names. We run a global network of domain name servers that are responsible for answering billions of queries every day. In running this network, we get probed, poked and attacked on a regular basis, sometimes in a small way and sometimes in a very huge way.

In addition, I spend time working with many of the people here on today's panel implementing solutions and working on technologies that enable the core of the Internet to "just work".

Many of the protocols used on the Internet were developed during a period when the number of infrastructure providers was limited and trust between each of these providers could be assumed. Hence, communication and interaction inside the DNS often presumes trust and sends sensitive data in a completely open manner. Credentials are sent "in the clear", DNS requests and replies are expected to be performed with fidelity and the authenticity of self-declared identities is taken for granted.

One of the biggest areas of concern for the Internet as a whole is the pervasive and malicious impact of Distributed Denial of Service (DDoS) attacks. A "denial-of-service" attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Attacks can be directed at any network device, including attacks on [routing](#) devices and [web](#), [electronic mail](#), or [Domain Name System servers](#). If an attacker mounts an attack from a single host it would be classified as a DoS attack. In fact, any attack against availability would be classed as a Denial of Service attack. On the other hand, if an attacker uses a thousand systems to simultaneously launch smurf attacks against a remote host, this would be classified as a DDoS attack.

The major advantages to an attacker of using a distributed denial-of-service attack are that multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, and that the behavior of each attack machine can be stealthier, making it harder to track down and shut down. These attacker advantages cause challenges for defense mechanisms. For example, merely purchasing more incoming bandwidth than the current volume of the attack might not help, because the attacker might be able to simply add more attack machines.

Users expect the DNS to respond properly, accurately and quickly – and to be available at all times. A DDOS attack can severely disrupt such expectations of service levels; in fact, a well orchestrated DDOS attack has the capability to shut down major parts of the Internet's core infrastructure by keeping it so busy answering bogus queries that it cannot handle real requests.

As more applications and systems expect the DNS to be present, ready and able to answer, the core stability of the DNS is threatened by concerted DDOS attacks against it. The size and scale of DDOS attacks have increased dramatically in the past 5 years – from a 10 Gigabits per second attack in 2005 to more than 50 Gigabits per second attack this year. Now, 50 Gigabits per second is itself a big attack – but the problem is that 50 Gigabits per second is only the tip of the iceberg.

Botnets have now proliferated – and botnets have become the largest way to execute DDOS attacks. Cloud computing has now spread to botnet operators themselves – you can now buy on-demand botnets on a pay as you go basis. The more you pay, the higher the size of your DDOS attack.

We no longer have to worry simply about large botnets that shut down large infrastructures – small botnets are now entirely capable of causing major disruptions for a country, or a service provider (like Gmail or Twitter) – while taking these down don't "shut down the Internet", they still have a massive impact on the use and reliability of the Internet.

The provisioning gap between bad actors and good players is increasing. It takes very little for a botnet operator to increase the size of their botnet by thousands of computers, magnifying the size of their attacks. It is far more difficult to provision and defend against such attacks – so the proportional change in the gap between the attacking side and the provisioning side is increasing dramatically. This is a cause for serious worry.

Solving the DDOS problem is a major factor for preserving the stability of the internet – and this cannot be done by regulation – it requires a significant level of investment, involvement by private operators, along with coordination with the public sector.