

Internet2 Abilene & REN-ISAC Arbor Networks Peakflow Identification and Response to DoS

International Trans-Atlantic Meeting
Dublin, Jan 18-19, 2006

Doug Pearson
Technical Director, REN-ISAC

Identifying DoS Sources

- Based on trace back of DoS traffic to Abilene router input interfaces we know what Connector or Peer network to attribute DoS activity to.
- In order to attribute activity further upstream, e.g. to a participant, NREN, or institution we need to know particulars about the Connector or Peer network.
 - Specifically need to know the methods and extent of spoofed source address filtering in the connected networks.

Spoofer Source Filtering

- On Abilene
 - Not done.
 - Fish issue with connectors and SEGPs.
- On others
 - GEANT, CA*net 4?

Reporting DoS Sources

- Report incidents to whom?
 - If there's no or incomplete filtering of spoofed sources by the connector or peer network then we can't count on source addresses being true, and need to report incidents to the NOC or security contact at the connector/peer network for trace back within that network.
 - If thorough spoofed filtering is practiced in the connector/peer then we can report the incidents directly to the participant or NREN security contact.
 - Does the connector/peer want copied anyway?

Reporting DoS Destinations

- Very useful to make report to the security team at the DoS destination:
 - Awareness, and
 - being the target of an attack often indicates the machine was previously hijacked or otherwise compromised.
 - REN-ISAC can make report directly to institution if contact points are known, otherwise will report to NREN CSIRT.
 - Likewise others can rely on REN-ISAC to forward incident reports when US participant contact points aren't known.