



PREDICT Anonymization Panel

The Tradeoffs of Anonymization

Stephen Schwab
SPARTA, Inc.



DDoS Experimenter's View

- **How is data useful to DDoS experiments?**
- **Two primary interests:**
 - DoS/DDoS ATTACKs from the wild
 - Background Traffic
- **Other interests:**
 - Inferring topology, peering relationships, etc.
 - Infrastructure impacts, e.g. DNS



Anonymization of Attacks

- **Subnet structure preservation**
 - How many source or destination address bits is the attacker randomizing, if any?
 - If multiple hosts contribute to an attack, are they sharing link bandwidth?
 - » Source addresses don't matter, only timing?
- **Novel attack discovery**
 - Flooding attacks are 1st generation
 - How does anonymization interact with confirmation of prevalence of other attacks



Anonymization of Background Traffic

- **Statistical Properties**
 - Distribution of source and destination addresses
- **Background may contain attacks on a higher layer protocol**
 - TCP: anonymize all data segments?
 - What about an attack carried out with legitimate TCP connections against an HTTP server?
 - » Repeated HTTP GETS for an expensive web page (requiring dynamic generation)
 - Distinguishing heavy load from flash crowds from intentional attack