Discussion of “DDOS and Worms” Session (SRUTI)

Vern Paxson (ICSI)

vern@icir.org

July 7, 2005

Abstracting the Three Talks

- ***Routing & Tunneling***:
  - Leverage name/path split to force traffic through upstream inspection points
  - Workable across domains because on top of existing inter-domain communication *and* fate-sharing of requests coming from the servers
  - Abstract detectors
  - Only effective for non-spoofed sources
    - *But* also argument for push towards deploying anti-spoof technology
  - I wonder about:
    - Relationship with CenterTrack, SOS, Pushback, PI, SIFF, I^3 (theme: implicit/explicit paths)
    - Bottlenecks

Abstracting, con’t

- ***Unwanted Backbone traffic***:
  - Leverage Zipf nature of where problems originate (e.g., heavy-hitter AS’s, ports)
    - ⇒ Solution fundamentally partial?
  - Concrete detector based on looking for an effective *partitioning plane*
  - I wonder about:
    - False positives (partition is probabilistic)
    - Obtaining ground truth - where to get labeled background traffic?
    - Vulnerability to spoofing / adversary analysis
    - Are ACLs fundamentally a scarce resource? Or are business relationships + service models more fundamental?

Abstracting, con’t

- ***Cooperative Containment***:
  - Thinking about defenses in quantifiable terms, cost/benefit tradeoffs
  - Leveraging the unwanted traffic’s <u>inefficiency</u>
  - Leveraging the unwanted traffic’s <u>wide scale</u>
    - E.g., implicit vs. explicit signaling
    - Dealing with untrusted parties via quorum
  - I wonder about:
    - Robust filter signature generation?
    - Efficacy for efficient (non-random-scanning) worms?
    - What if the adversary is content with < T networks?
    - How much of the worm problem is fundamentally different from other unwanted traffic due to global scale?