Threats (Green=in-scope, black=under discussion, red=out-of-scope)

- Threats to underlying infrastructure
  - System failure
  - Government interventions
  - Physical
  - Fragmentation of the root -- SAC 9
  - (FY12) ?? expand
  - Depletion of IPv4 address pool -- SAC 12
  - Business failure
    - Scope
      - Doubtful that the failure of a registry (perhaps with the exception of .com/.net) will have a substantial impact on the DNS
- Direct Attacks
  - DDOS
  - Packet Interception
  - Recursive vs authoritative nameserver attacks
  - Authority or authentication compromise
  - Data poisoning (MITM, Cache)
  - IDN attacks (lookalike characters etc. for standard exploitation techniques)
  - Malicious or unintentional (erroneous) alteration of DNS configuration information
  - Footprinting
    - Scope
      - A behavior, a threat-vector in some cases
      - A threat to individual machines/systems -- focused/limited threat – not likely to cause widespread instability
  - Authenticated Denial of Domain Name (RFC 3833)
    - Scope
      - A behavior, a threat-vector in some cases
      - A threat to individual machines/systems -- focused/limited threat – not likely to cause widespread instability
  - Malicious or unintentional (erroneous) alteration of contact information SAC
    - Scope
      - A behavior, a threat-vector in some cases
      - A threat to individual machines/systems -- focused/limited threat – not likely to cause widespread instability
- Indirect attacks
  - Email/spam
  - Registration abuse -- front-running
    - Scope
      - A problem at the 2nd level, not a threat to the DNS
      - Some question as to whether this happens much at all
  - Registration abuse -- cybersquatting
    - Scope
      - A problem at the 2nd level, not a threat to the DNS
  - WHOIS abuse -- harvesting WHOIS data for spam
    - Scope
      - A problem at the 2nd level, not a threat to the DNS
      - A policy issue, but not a threat to the DNS
      - IETF is discussing at this time -- we may want to monitor this discussion
  - WHOIS abuse -- harvesting personal contact information from domain name registration records -- SAC 14
    - Scope
      - A problem at the 2nd level, not a threat to the DNS