- Threats
  - Threats
    - Threats to underlying infrastructure
      - Business failure
      - System failure
      - Government interventions
      - Physical
      - Depletion of IPv4 address pool -- SAC 12
      - Fragmentation of the root -- SAC 9
      - (FY12) ?? expand
    - Direct Attacks
      - DDOS
      - Packet Interception
      - Recursive vs authoritative nameserver attacks
      - Authority or authentication compromise
      - Domain name hijacking/theft - SAC 7
      - Registrar impersonation phishing attacks -- SAC 28
      - Data poisoning (MITM, Cache)
      - Footprinting
      - Fast Flux
      - IDN attacks (lookalike characters etc. for standard exploitation techniques)
      - Authenticated Denial of Domain Name (RFC 3833)
      - Gain control of account user/password
      - Malicious or unintentional (erroneous) alteration of DNS configuration information SAC 44
      - Malicious or unintentional (erroneous) alteration of contact information SAC 44
    - Indirect attacks
      - Email/spam
      - Registration abuse -- front-running
      - Registration abuse -- cybersquatting
      - WHOIS abuse -- harvesting WHOIS data for spam
      - WHOIS abuse -- harvesting personal contact information from domain name registration records -- SAC 14
  - Vulnerabilities
    - Operational issues
      - Business/technical process vulnerabilities
      - Infrastructure vulnerabilities
    - Managerial choices/issues
      - Lack of visibility and understanding by decision-makers
      - Inadequate documentation of DNS architecture and operations (SAC 49)
      - Inadequate funding (for infrastructure, training, etc.)
      - Inadequate continuity planning for recovering from DNS outages
      - DNSSEC
      - Not following best practices
    - Vulnerability of DNS software, OS, etc.
      - registrar automation patterns/behaviors
      - Content provisioning exposure -- eg Akemi -- if credentials leak, there's broad exposure -- registrar account credentials
      - Inaccurate registration contact information
      - Single-factor authentication
      - Time to live
      - Weaknesses of DNSSEC (RFC 3833)
      - Securing DNS Dynamic Update (RFC 3833)
      - Securing DNS Zone Replication (RFC 3833)
      - Wildcards
      - high value names
    - Bad players
      - Insiders
      - Organized crime
      - Geo-political groups
      - Rogue elements
      - Nation states
  - Possible hierarchies
  - Action-items