- **Main Topic**
- **Action-items**
  - Clarifications
    - Mark
      - Leverage the DNS and unique identifiers (such as botnets, denial of service attacks, social engineering attacks) for fraud, malicious conduct or route-hijacking attacks
  - **Impacts**
  - **Mitgation**
- **Threats**
  - Threats on the underlying infrastructure. May include:
    - Disasters
      - TLD and registrar failure
      - Natural disasters
    - Authority or authentication compromise
    - Government interventions
    - Physical
      - Terrorism
      - Facility security
    - External events (non Internet protocol events?)
      - Acts of war/terror
      - Natural disaster
      - Physical disasters
    - (FY12)
  - Direct Attacks
    - Cache poisoning attacks
      - Kaminsky
      - Kaspureff
    - Recursive vs authoritative nameserver attacks
    - DDOS attacks
      - Botnets
    - Fast Flux
    - DOS
      - Hackers
    - Man in the middle
    - IDN attacks (lookalike characters etc. for standard exploitation techniques)
    - Targeted attack
      - DDOS
      - Hacking/penetration
      - Data poisoning (MITM, Cache)
    - Reflection attacks
  - Indirect attacks
    - Email/spam
      - IPv6 -- Spammers hopping from IP to IP -- causing huge numbers of lookups -- volume related threats (perhaps unintentional) -- also may break normal DNS caching (whicha assumes repeated requests for the same thing)
      - Issues around reverse DNS for SMTP servers
      - Botnets
      - Collateral damage
      - Load
  - Societal threats?
    - Spoofing
    - Alternate DNS roots
    - DNS blocking
    - Political
      - State-sponsored
      - Hacktivism
  - Background materials on threats
    - SSAC Reports
      - http://www.icann.org/en/committees/security/sac040.pdf and http://www.icann.org/en/committees/security/sac044.pdf
    - RFC - 3833 -- user, app, OS, ISP, DNS, registrar, registrant, registry -- threat analysis to the domain name system - http://www.ietf.org/rfc/rfc3833.txt
- **Threats**
  - Vulnerabilities
    - Operational errors
      - Informality of some processes
    - Managerial choices/issues
      - Lack of visibility and understanding by decision-makers
      - Inadequate funding (for infrastructure, training, etc.)
    - Implementation errors (hardware and software)
    - Bugs
    - Single point of failure
      - Topology
      - Service providers
      - Software
      - Hardware
      - Geo location
      - Infrastructure (electricity, fiber, etc.)
    - Supporting infrastructure (insufficient SLA's, support, etc)
      - Rapid change
    - Homogeneity (software, hardware, etc) -- small gene pool, one vulnerability could have broad impact
    - Poor design (hardware and software)
    - Vulnerability of DNS software, OS, etc.
    - Scalability issues
    - Content provisioning exposure -- eg Akemi -- if credentials leak, there's broad exposure -- registrar account credentials
    - Split DNS
    - DNSSEC private key exposure
    - Bad players
      - Organized crime
      - Geo-political groups
      - Rogue elements
      - Nation states
  - Possible hierarchies
    - Layers
      - Threats that leverage the DNS
      - Threats against the underlying infrastructure
    - Temporal
      - Attacks on the protocol layer below the DNS
    - Direct vs indirect
    - Needs to border DNS
      - so the several recent papers by eff, zhang and others on isp monitizing synthetic return/content modification
      - No single authoritative DNS (eg alternate root-servers) , lack of DNS response integrity
      - alternate root, strings appearing in other configurations not supported in the global root
      - Possible extensions of carrier-grade NAT
    - Question from the group: "What is the perspective of threat description?"
      - RFC - 3833 -- user, app, OS, ISP, DNS, registrar, registrant, registry -- threat analysis to the domain name system
      - Picture
      - Registrant <--> Registrar) Compromised credentials (Phishing, Key logger, social engineering, a.o.)
      - Registrar <--> Regisrty) Compromised credentials, DDOS
      - Registry <--> DNS) DDOS
      - DNS <--> End user) Spoofing, poisoning
      - ALL) MIM (Man in the middle)