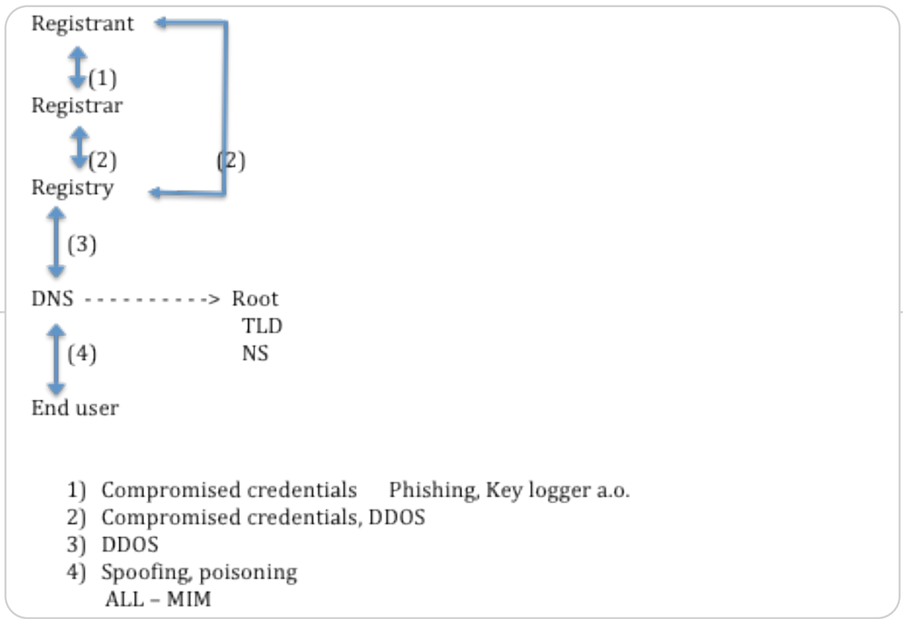
Threats

- **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
- **Threats**
  - Threats on the underlying infrastructure. May include:
    - TLD and registrar failure
    - Disasters
    - Authority or authentication compromise
    - Government interventions
    - (FY12)
  - Direct Attacks
    - Cache poisoning attacks
    - Recursive vs authoritative nameserver attacks
    - DDOS attacks
    - DOS
    - IDN attacks (lookalike characters etc. for standard exploitation techniques)
    - 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
  - Vulnerabilities
    - Bugs
    - Vulnerability of DNS software, OS, etc.
    - Split DNS
  - External events (non Internet protocol events?)
    - Acts of war/terror
    - Natural disaster
    - Physical disasters
  - Possible hierarchies
    - Layers
      - Threats that leverage the DNS
      - Threats against the underlying infrastructure
    - Temporal
      - Attacks on the protocol layer below the DNS
    - 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
- **Olivier**
  - Physical
    - Terrorism
    - Facility security
  - Single point of failure
    - Topology
    - Service providers
    - Software
    - Hardware
    - Geo location
    - Infrastructure (electricity, fiber, etc.)
  - Targeted attack
    - DDOS
    - Hacking/penetration
    - Data poisoning (MITM, Cache)
  - Alternate DNS roots
  - DNS blocking
  - Political
    - State-sponsored
    - Hacktivism
  - Picture
- **???**
  - Poor design (hardware and software)
  - Natural disasters
  - Bad players
    - Organized crime
    - Geo-political groups
    - Rogue elements
  - Nation states
  - Implementation errors (hardware and software)
  - Operational errors
  - Scalability issues
  - Rapid change
  - Informality of some processes
  - Inadequate funding (for infrastructure, training, etc.)
  - Lack of visibility and understanding by decision-makers
  - Picture
- **Roy**
  - Botnets
  - Cache poisoning
    - Kaminsky
    - Kaspureff
  - Spoofing
  - M+M
  - Fast Flux
  - Operational errors
  - Supporting infrastructure
  - Hackers
  - Homogeneity
  - Content provisioning exposure
  - DNSSEC private key exposure
  - Question from the group: "What is the perspective of threat description?"
  - Picture
- **Katrina**
  - 

  - 1) Compromised credentials (Phishing, Key logger, a.o.)
  - 2) Compromised credentials, DDOS
  - 3) DDOS
  - 4) Spoofing, poisoning
  - ALL) MIM (Man in the middle)
  - Picture