Threats

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 on the underlying infrastructure. May include:
  - TLD and registrar failure
  - Disasters
  - Authority or authentication compromise
  - Government interventions
  - (FY12)
- Needs to border DNS
- Cache poisoning attacks
- Recursive vs authoritative nameserver attacks
- Reflection attacks
- Vulnerability of DNS software, OS, etc.
- DDOS attacks
- Physical disasters
- IDN attacks

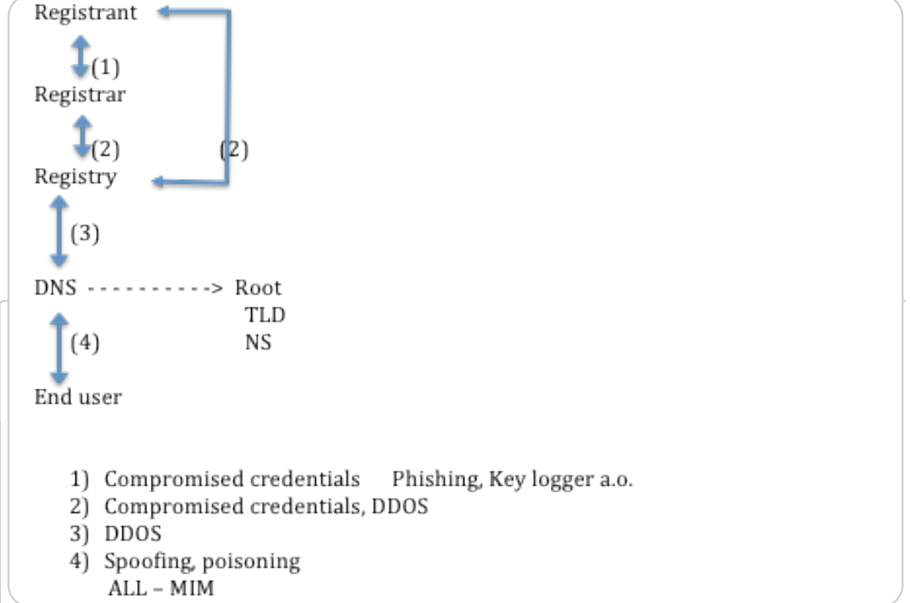
Roy

- Natural disaster
- Acts of war/terror
- Bugs
- DOS
- Spam
- 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

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

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

???

- 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