DNSsec in (medium/small) ccTLD Registries

ICANN 48, Buenos Aires, Argentina

@oscarrobles

DNSsec helps to mitigate some risks

- False zones information (Forgery/Falsification)
  - DNS information obtained by the resolvers is different from authoritative answers.
    - Mainly in wireless networks
- DNS Cache Poisoning (man in the middle)
  - Flood to a DNS resolver with false information and eventually may match actual DNS requests and will get the false answer.

- As a result, end users will be directed to unintended URLs.

(non) Typical DNSsec concerns

- Increase number of DNS packets (because of its size), increasing DNS traffic.
- CPU capacity to sign zones at DNS servers level.
- Medium and Small ccTLD Registries (with limited resources)
  - DNS operation turns into a more complex task with DNSsec.
  - That risk magnitude may be higher than current security concerns.
    - Difference strives that the former may compromise **the whole DNS zone for the whole Internet**.
    - The later may compromise specific RR's for specific networks.

Different times

- DNSsec was developed in the mid 90’s, still it covers current security concerns on some behaviors.

- The challenge is to keep DNS resilient to attackers, home and abroad.
- Recent IETF consensus
  - http://www.ietf.org/blog/2013/11/strengthening-the-internet/
- Competitive disadvantage
  - From the business perspective, there will be hundreds of new gTLDs that will have DNSsec implemented (forced by contract).

DNSsec .MX

- Project started: July 2012
- Testing started: May 2013
- DNSsec deployment: March 2013
  - Registrars
- .MX signing zone: May 2014

Challenges to Medium and Small Registries

- Operational Complexity vs. Security Threats
- Lack of Registrar interest to develop it
- Growth on security risks
- Growth of Government concerns on security online