DNSSEC

VeriSign Naming & Directory Services
ICANN Kuala Lumpur
July 2004
DNS Security Extensions (DNSSEC)

+ DNSSEC uses public key cryptography and digital signatures to provide:
  + **Data origin authentication**
    + E.g., “Did this DNS response really come from a.gtld-servers.net?”
  + **Data integrity**
    + E.g., “Did an attacker—a man-in-the-middle—modify this DNS response?”
  + **Bottom line:** DNSSEC offers protection against spoofing of DNS data
What DNSSEC Does Not Do

+ DNSSEC does not:
  + Provide any confidentiality for DNS data
    + I.e., no encryption
    + Assumption: The data in DNS is public
  + Address attacks against the name server itself
    + Denial of service
    + Implementation vulnerabilities
    + Etc.
DNSSEC killer app(?) : secure data store

+ Spamt mitigation
  + DNSSEC will not stop it outright but indirectly through output of IETF MARID WG
    + MARID WG focus is using DNS to ID valid originating mail senders
    + Focus of attack for spammers will then be to spoof DNS to get spam through

+ Opportunistic encryption
  + Want to use IPSEC encryption with hosts but do not know key
  + Use DNS to store/retrieve the public key

+ Secure shell
  + Use to find hosts’ SSH public keys
  + Would replace caching mechanism that is in place today

+ Tomorrow’s applications…
  + Information store for secure routing information?
  + ??
Infrastructure Impacts of DNSSEC
Implementing DNSSEC in \textit{com/net}

+ Extensions to EPP supporting DNSSEC provisioning
+ Update registry database to include DNSSEC-related information
+ Acquire cryptographic hardware
+ Define process to generate and maintain keys
+ Implement incremental signing process
+ Update zone file generation process
+ Update ATLAS (authoritative name server platform)
DNSSEC Provisioning

+ Registrant generates a public/private key pair for a zone
+ Registrant signs the zone with the private key
+ Registrant sends the zone’s public key to the registrar
+ Registrar sends registrant’s key to the registry
+ Registry puts registrant’s key hash (DS) in the TLD zone
+ Registry signs the TLD zone
+ Registry publishes signed TLD zone
Pilot Programs

+ [www.dnssec.verisignlabs.com](http://www.dnssec.verisignlabs.com) demonstrated Opt-In
  + Opt-In did not advance in the IETF and this pilot is now defunct
+ [www.dlv.verisignlabs.com](http://www.dlv.verisignlabs.com) demonstrates an alternative called DNSSEC Lookaside Validation (DLV)
  + Protocol extension developed by Internet Systems Consortium (BIND maintainers)
  + DLV uses third-party for authentication rather than standard DNSSEC’s top-down model
+ Comprehensive DNSSEC pilot for .Net
  + Ready in September
  + Participants make local change to access DNSSEC-signed version of .Net
DNSSEC Consortium

- Most DNSSEC deployment meetings have focused on:
  - Protocol deficiencies
  - Securing the DNS root
  - Deployment strategies

- The **DNSSEC Consortium** will be focused on:
  - Encourage application developers to design, develop and launch the most meaningful solutions demanded by the marketplace
  - Getting all the DNS players (registries, registrars, OS providers, DNS software vendors, application developers, etc.) together to:
    - Share views on DNSSEC
    - Share deployment plans
    - Coordinate rollout dates
    - Compile a library of APIs, white papers, best practice documents, etc

- First meeting in San Diego in August before IETF