DNSSEC at the Root: Opening the Door to Opportunity

Securing the DNS: Towards a more secure Internet, Stockholm

29 July 2009

Rick Lamb

The Road to Signing the Root

- >Decade of protocol development
- Trailblazing work by .SE
- Consistent community pressure
- Many signed root test beds
- pr, .br, .bg, .cz, .gov, .org, .th
- experience despite FUD
- Kaminsky
- Proposals
- NOI
- DoC Requirements
- Intense cooperative effort VeriSign ICANN DoC
- Target: interim signed root by end of year
- ICANN's new CEO has stated the DNSSEC effort is truly important

What DNSSEC Does Not Solve

- All the Internet's ills
- Social engineering attacks
- Domain name hijacking
- SPAM
- DDOS
- Ensure accuracy of content

Threats that DNSSEC Addresses

- Cache Poisoning
- Pharming
- DNS redirection attacks or hijacking
- Complementary to SSL

What does Signing the Root do?

- Removes deployment barriers
- Simplicity of a “single” key
- Compromise recovery
- Leads by example

But Wait…There's More…

- Unlike other attempts at global authentication systems,
  - with DNSSEC deployed at the root..
  - TLD's are unencumbered to build into this infrastructure.
- Removes a barrier to a global authentication infrastructure
- DNS is already a public infrastructure.
  - DNSSEC adds the "K" to this PKI - Kaminsky
- A global alternate source of trust and authentication
- And platform for innovation and new products

Envisioned for Many Years

- For example:
  - X.509/Certs (rfc2538/4398)
  - DKIM (rfc4871)
  - SSHFP (rfc4255)
  - IPSECKEY (rfc4025)
  - Other ??

Summary

- DNSSEC is happening
- A tool for cybersecurity
- A rare opportunity
- Signing the root clears the way for widespread DNSSEC deployment which would not only secure the Internet's phonebook, but also create a platform for innovation and cross- organizational / international cooperation in cybersecurity.