DNSSEC: General Introduction

James M. Galvin, Ph.D.
Director Strategic Relationships and Technical Standards

ISOC Philadelphia Chapter
11 June 2010
Who is Afilias?

- **10 years of experience** in critical Internet infrastructure
- Best known for domain name registry services in **support of 15 million domains** across 15 TLDs
- Diverse DNS Network handling **billions of queries** daily
- Launched Managed DNS services in Feb 2009
DNSSEC capable

• Afilias signed the .ORG registry, on behalf of PIR in June 2009.
  – First large generic TLD signed
• Running DNSSEC testbed for registrars and registry customers
• Beta-testing 1-Click DNSSEC product, that would provide managed DNSSEC services for key management, distribution and rollover
1. What problems does DNSSEC solve?
2. Industry Context
3. A DNSSEC Primer
4. Key Management Primer
1. What problems does DNSSEC solve?

Why Do Domain Name System Security Extensions (DNSSEC) Matter?
Without DNSSEC…

When you visit a web site, or send an email, can you be sure you are communicating with the server that you think you are?
TLS and DNSSEC benefits

- **TLS**
  - Data
  - Encryption

- **DNSSEC**
  - Signed
  - Guaranteed not tampered
  - Authentication
  - Integrity

**DNSSEC protects...**

Users from **DNS data** tampered by or originating from malicious actors
1. A DNS resolver sends a DNS query and accepts the first response it receives.
1. A DNS resolver sends a DNS query and accepts the first response it receives.

2. If a malicious system returned an incorrect response, any resolver will use until its cache expired.
ISP risks

A broader-based attack
When a malicious agent attacks your ISP’s iterative resolver it affects all users of the ISP

DOMAIN NAME SYSTEM

When a malicious agent attacks your ISP’s iterative resolver it affects all users of the ISP.

ISP

CACHE

www.trustus.info = 192.172.3.4

192.168.16.2

www.trustus.info

SERVER

192.172.3.4

get

www.trustus.info
DNS Resolution + DNSSEC

- DNSSEC adds security to the DNS
  - Signatures
  - Keys to validate them
- Keys exist at various levels
  - Root key is the trusted authority
  - Registries and registrants have own keys to sign data
  - Resolvers retrieve keys to check signatures
- DNS data is protected
  - It does not matter what server or resolver provides the data
What are the Benefits?
What is the demand?
What is the Industry context?
## DNSSEC benefits by role

<table>
<thead>
<tr>
<th>End User</th>
<th>Registrant</th>
<th>Registrar</th>
<th>Registry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gain confidence of reaching the intended website</td>
<td>Fraud mitigation</td>
<td>Comply with new industry standards</td>
<td>Meet new industry standards</td>
</tr>
<tr>
<td>Backwards compatible with those not using DNSSEC but they continue to be at risk</td>
<td>Greater brand protection</td>
<td>Meet Registrant demands for increased domain security</td>
<td>Meet Registrar demands for increased security of their registrants’ domains</td>
</tr>
</tbody>
</table>
The demand for DNSSEC?

- A mix of pioneers, early adopters and legislated compliance
- In the early stages for user awareness

Barriers
- Complexity
- Costs

Incentives
- Signing TLDs: .ORG, .GOV
- New hw & sw solutions

© Afilias Limited
www.afilias.info
Recent news reports of DNS attack events ask:

“Would DNSSEC have mitigated the attack?”

- Neustar signed .US
- Neustar signs .BIZ in 2Q2010
- VeriSign signs .EDU in 3Q2010
- VeriSign signs .NET in 4Q2010 & .COM in 1Q2011
- .ORG signed delegations
- .ORG Root signed delegations