DNSSEC
DNS Security Extension Deployment in .ORG

Monday 23 June 2008
ICANN Paris
Agenda

» PIR Implementation Approach
» RSTEP Report Outcome
» Risk Analysis
» What We Are Evaluating
» Milestones
Our Approach

» Motivation - Do the right thing not just for .ORG but for the Internet at large:
  • A secure DNS is a fundamental layer for future development
  • To do this, a gTLD has to come forward
    – implementation of DNSSEC at gTLD level will enable awareness, education and adoption, →
    – So…the next generation Internet features a secure DNS

» Approach – Collaborate, Learn, Share
  • Learn: ccTLDs
  • Collaborate: RIPE, Afilias, Nominet
  • Share: DNSSEC Adoption Survey
RSTEP Report Outcome

» Overall
  – RSTEP review team gave thumbs up to our proposal
  – Finite but manageable adverse risk to security and stability of the .ORG zone

» Key Observations
  – Many issues solved with a signed root
  – Registrar adoption allows for better user choice
  – Suggests possible use of multiple KSKs
    • PIR is evaluating the risk vs. benefit of multiple keys
  – Concerned about “stopping DNSSEC” if needed
    • Proposes implementing RFC 5011
    • In our opinion – this does not solve the problem, since a complete key set compromise would still need a “full stop”
Risk Analysis

» Four categories of risks:

– *Not* inherent or specific to DNSSEC

– Are specific to DNSSEC but whose *probability is so low*, it does not materially impact our plans

– Are specific to DNSSEC, but until we implement we will not know

– Are specific to DNSSEC and we plan to adjust our plan accordingly
# Risk Analysis

<table>
<thead>
<tr>
<th>#1</th>
<th>#2</th>
<th>#3</th>
<th>#4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not specific to DNSSEC <em>(no action needed)</em></td>
<td>Yes...probability = lightning striking me as I speak <em>(not a real risk)</em></td>
<td>(Will not know full measure until we implement) <em>(normal pre-op testing)</em></td>
<td>(Valid – we will evaluate our plan) <em>(useful work to be done)</em></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3.4.1: Transmission of DS records is exactly the same as transmission of other registrant data</th>
<th>3.5.6: PIR will be using HSM. This is a mature technology and does not fail in a way that exposes private keys.</th>
<th>3.2: Proper operation of the .ORG domain should be presumed. Configuration errors in browsers will need to be ironed out for everyone</th>
<th>3.4.5: At least two registrars enabled before there is formal operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.4.2: PIR will not require key change when registrar changes</td>
<td>3.4.6: Unlikely and easily detectable. Registrars will be required to be responsive</td>
<td>3.5.5: Registrants may need to improve their own operation or obtain assistance. Education will help</td>
<td></td>
</tr>
<tr>
<td>3.5.4: Signing interval of DS consistent with TTL</td>
<td>3.5.3: Unlikely and easily detectable. Issues will be taken care of during normal shakedown</td>
<td>3.6.2: Report suggests a testing site for people to try out whether their configuration properly interacts.</td>
<td></td>
</tr>
</tbody>
</table>
## Risk Analysis (cont.)

<table>
<thead>
<tr>
<th>#1</th>
<th>Not specific to DNSSEC <em>(no action needed)</em></th>
<th>#2</th>
<th>Yes...probability = lightning striking me as I speak <em>(not a real risk)</em></th>
<th>#3</th>
<th>Will not know full measure until we implement <em>(normal pre-op testing)</em></th>
<th>#4</th>
<th>Valid – we will evaluate our plan <em>(useful work to be done)</em></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.5.7: Zone signing has already been tested</td>
<td>3.6.5: DOS potential is not a threat as the signed answers are still much shorter than 4096 byte TXT record.</td>
<td>3.6.1: Most, if not all of this should be dealt with during shakedown period</td>
<td>3.6.7: PIR will work with trust anchor repository (TAR) operators to help the community build a robust scheme.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.4.3: Fast publication when the key changes is already part of PIR’s operation.</td>
<td>3.6.6: It’s not clear that redundant info in the WHOIS record regarding algorithms used would help. It might create additional complexity and potential inconsistency.</td>
<td>3.6.4: Additional load is limited and manageable</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.6.3: Multiple NS operators serve the zone</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
What We’re Evaluating

» **Key Management**
  • RSTEP suggests using multiple KSKs to mitigate bogus zone problem

» **Key Rollover Policies**
  – We believe our policies lead to good security
    • ZSKs will be updated at least monthly
    • KSKs will be updated at least yearly
  – The frequent updates cause some stability concerns
    • We intend to address by a limited scope launch, user and registrar education
    • We need feedback from network operators, registrars, and others on the expected impact of our rollover policies

» **Use of Trust Anchor Repositories (TAR)**
  – We will place the keys for .ORG in the IANA DS registry
  – We do not currently plan to use DLV

» **Registrar/Registrant adoption**
  – We are signing up registrars now to ensure sufficient adoption exists
  – Testing site may help
A Controlled Launch

- June 2008
  - RSTEP Response
- Q4 2008 (estimated)
  - BIND NSEC3 compatibility release
  - HSM Integration
- Q1 2009 (estimated)
  - Friends & Family signed zones (pir.org, isoc.org, afilias.org, etc)
- Q3 2009 (estimated)
  - Expanded Friends & Family (based on results of F&F)
- 2010 (estimated)
  - Mainstream availability - Monitor, evaluate, then when advisable release to whole zone
Questions?

araad@pir.org
Appendix
Registrars

» New Registrar Tool Kit for DNSSEC
  – Adds DNSSEC EPP transactions (RFC 4310)
» Registrars Do Not Have to use
  – But MUST pass OT&E if they do
» Registry assumes all data is correct and valid
  – Similar to other WHOIS and DNS data
» To transfer, gaining registrar must be DNSSEC-ready
  – or registrant can wipe DNSSEC info
EPP Server

» Modified for DNSSEC
  – Adds DNSSEC EPP transactions (RFC 4310)
Registry Database

- Stores DS information
- Holds MaxSigLife
  - Currently set to default of 10 days
Zone Signing

» Using HSM for key generation and zone signing
  – FIPS 141-2 compliant

» Will sign domain names as they come through
  – Full zone re-sign will be fed through as quickly as possible
Name Servers

» Will Support NSEC3
  – Currently Using NSD and BIND
» Servers already have enough capacity
  – Hooray for opt-out!
Ancillary Functions

» PIR Website
  – Will have public information for validators

» Email list (read-only)
  – Notifies everyone when TA must be updated
IANA

» Will Update DS on each change
  – Using new IANA DS Registry
    • (Once it's up and running)
  – Also once the root is signed
» Admins should sign up for email list
  – Once it's ready
» PIR preparing help docs for admins to configure TA info
» Will need to update at least once / year