5011 Security Considerations

Wes Hardaker <hardaker@isi.edu>
Warren Kumari <warren@kumari.net>

Issues from Last Call: Ed Lewis

1. “The audience of this document (namely the targetted operators [ICANN]) has not participated in the review of the document”
    - **STATUS: The authors have had extensive conversations with all levels of ICANN staff**
2. “Trust Anchor” usage is incorrect
    - Resolution: Agreed and document terminology fixed
    - EG “Trust Anchor Publisher” => “PEP Publisher” (and other fixes)
    - **STATUS: Fixed**
3. “The document begins to co-mingle validation with trust anchor management”
    - Agreed -- all terminology cleaned up; but do note that DNSSEC validation is required
    - **STATUS: Fixed**
4. “Not worth our time”
    - “Low ROI”, “unsupported Safety Margin”
    - **More on this later...**

Issues from Last Call: Paul Hoffman

1. “... or with an additional section on looking at timing from a second perspective” [re: MSJ timing]
    - **STATUS: Additional section added**

Issues from Last Call: Michael StJohns

1. Timing: "When is it safe for me to revoke all of the older trust anchor keys?"
    - IE, “at what time of what day” vs “how long from now”
    - **STATUS: current document contains both calculations** *(see also: Paul Hoffman)*
2. “The safety factor is there primarily to deal with network outages AT THE RESOLVER and is a SWAG”
    - Suggests: safetyFactor ::= retryInterval * (5 + Log2(N))
    - retryInterval = MAX(1 hr, MIN (1 day, 0.1 * origTTL, 0.1 * expireInterval)
    - And suggests 5+Log2(N) is 28 to cover 99.99% of 10M resolvers
    - **more on this later...**

Draft-07

Draft-08 (TBD)

Big Question #1: Should This Be Published At All?

Paul Hoffman: Yes

Michael StJohns: Unknown

Ed Lewis: No

Authors: Yes (of course)

You: ????

Big Question #2: What about the safety margin?

- Some folks worried about network delays and race conditions
- Some folks thinks it adds “slop” to an otherwise precise equation
- Choice:
  a. Don’t add a safety margin value and keep it precise
  b. Figure out the right value of slop to put in

- Current safetyMargin choices:
  a. safetyMargin = MAX (1.5 hours, 2 * MAX(TTL of all records))
  b. safetyMargin = (5 + Log2(N)) * MAX(1 hr, MIN (1 day, 0.1 * origTTL, 0.1 * expireInterval)
  c. ???