draft-ietf-dnsop-rfc5011-security-considerations

Wes Hardaker, Warren Kumari

2017-07-16

Outline

Math Reminder – 5011

$$queryInterval = MAX \begin{cases} MIN \begin{cases} \frac{DNSKEY\ \ RRSIG\ \ Signature\ \ Validity}{2} \\ \frac{TTL\ \ of\ \ K_{old}\ \ DNSKEY}{2} \\ 15\ days \end{cases} \\ 1\ hour \end{cases}$$

Math Reminder – 5011-security-considertions

$$
\begin{aligned}
addWaitTime = \; & addHoldDownTime \\
& + DNSKEY\ RRSIG\ Signature\ Validity \\
& + queryInterval \\
& + 2 \bullet MAX(TTL\ of\ all\ records)
\end{aligned}
$$

Math Reminder – 5011-security-considertions

$$
\begin{aligned}
addWaitTime = \; & addHoldDownTime \\
& + DNSKEY\ \ RRSIG\ \ Signature\ \ Validity \\
& + MAX \left\{ \begin{array}{l} MIN \left\{ \begin{array}{l} \frac{DNSKEY\ \ RRSIG\ \ Signature\ \ Validity}{2} \\ \frac{TTL\ \ of\ \ K_{old}\ \ DNSKEY}{2} \\ 15\ days \end{array} \right. \\ 1\ hour \end{array} \right. \\
& + 2 \bullet MAX(TTL\ \ of\ \ all\ \ records)
\end{aligned}
$$

Issue #1: Revocation from 5011

2.4.2. Remove Hold-Down Time

The remove hold-down time is 30 days. This parameter is solely a key management database bookeeping parameter. Failure to remove information about the state of defunct keys from the database will not adversely impact the security of this protocol, but may end up with a database cluttered with obsolete key information.

Issue #1: Revocation from 5011

- 5011 states revocation is immediate
- 30-day timer is purely "bookkeeping"
- Thus, the math is actually different
  - (and shorter in time)

$$remWaitTime = \cancel{addHoldDownTime} + DNSKEY\ RRSIG\ Signature\ Validity + MAX\left\{ \begin{array}{l} MIN\left\{ \begin{array}{l} \frac{DNSKEY\ RRSIG\ Signature\ Validity}{2} \\ \frac{TTL\ of\ K_{old}\ DNSKEY}{2} \\ 15\ days \end{array} \right. \\ 1\ hour \end{array} \right. + 2 \bullet MAX(TTL\ of\ all\ records)$$

Issue #1: Revocation

- 5011 states revocation is immediate
- 30-day timer is purely "bookkeeping"
- Thus, the math is actually different
  - (and shorter in time)

$$remWaitTime =$$

$$DNSKEY\ RRSIG\ Signature\ Validity$$

$$+ MAX \begin{cases} MIN \begin{cases} \frac{DNSKEY\ RRSIG\ Signature\ Validity}{2} \\ \frac{TTL\ of\ K_{old}\ DNSKEY}{2} \\ 15\ days \end{cases} \\ 1\ hour \end{cases}$$

$$+ 2 \bullet MAX(TTL\ of\ all\ records)$$

Current KSK data: adding

addHoldDownTime	30 days
Old DNSKEY RRSIG Signature Validity	21 days
Old DNSKEY TTL	2 days

$$
\begin{aligned}
addWaitTime = \; & addHoldDownTime \\
& DNSKEY\ RRSIG\ Signature\ Validity \\
& + MAX \left\{ \begin{array}{l} MIN \left\{ \begin{array}{l} \frac{DNSKEY\ RRSIG\ Signature\ Validity}{2} \\ \frac{TTL\ of\ K_{old}\ DNSKEY}{2} \\ 15\ days \end{array} \right. \\ 1\ hour \end{array} \right. \\
& + 2 \bullet MAX(TTL\ of\ all\ records)
\end{aligned}
$$

Current KSK data: adding

addHoldDownTime	30 days
Old DNSKEY RRSIG Signature Validity	21 days
Old DNSKEY TTL	2 days

$$
\begin{aligned}
addWaitTime = \; & 30 \\
& + 21 \\
& + MAX \left\{ \begin{array}{l} MIN \left\{ \begin{array}{l} \frac{21 \ days}{2} \\ \frac{2 \ days}{2} \end{array} \right. \\ 15 \ days \\ 1 \ hour \end{array} \right. \\
& + 2 \bullet 2 \ days
\end{aligned}
$$

Current KSK data: adding

addHoldDownTime	30 days
Old DNSKEY RRSIG Signature Validity	21 days
Old DNSKEY TTL	2 days

$$
\begin{aligned}
addWaitTime = \; & 30 \\
& + 21 \\
& + MAX \left\{ \begin{array}{l} MIN \left\{ \begin{array}{l} 11.5 \; days \\ 1 \; days \\ 15 \; days \end{array} \right. \\ 1 \; hour \end{array} \right. \\
& + 4 \; days
\end{aligned}
$$

Current KSK data: adding

addHoldDownTime	30 days
Old DNSKEY RRSIG Signature Validity	21 days
Old DNSKEY TTL	2 days

$$
\begin{aligned}
\mathit{addWaitTime} = \; & 30 \\
& + 21 \\
& + 1 \; \mathit{days} \\
& + 4 \; \mathit{days} \\
& = \; 56 \; \mathit{days}
\end{aligned}
$$

Current KSK data: revocation

addHoldDownTime	30 days
Old DNSKEY RRSIG Signature Validity	21 days
Old DNSKEY TTL	2 days

$$\begin{aligned} \mathit{remWaitTime} = {} & \cancel{30} \\ & + 21 \\ & + 1\ \mathit{days} \\ & + 2 \bullet 2\ \mathit{days} \end{aligned}$$

Current KSK data: revocation

addHoldDownTime	30 days
Old DNSKEY RRSIG Signature Validity	21 days
Old DNSKEY TTL	2 days

$$
\begin{aligned}
\mathit{remWaitTime} = & \\
& + 21 \\
& + 1 \ \mathit{days} \\
& + 2 \bullet 2 \ \mathit{days} \\
& = \ 26 \ \mathit{days}
\end{aligned}
$$

Issue #2: Interval vs Wall Clock

- addHoldDownTime = 30 days from publication
- sig expiration = wall clock time *(date/time stamp)*
- Equations could be structured as either:
  - addWaitTime = ...
  - addSafeClockTime = ...

Draft Status

- Update imminent
- Ready for WG last call?