rpkimaxlen update - IETF 110

Ben Maddison

2021-03-10

draft-ietf-sidrops-rpkimaxlen

document status and updates

Authors:

- Yossi Gilad
- Sharon Goldberg
- Kotikalapudi Sriram
- Job Snijders
- Ben Maddison

Recap

- Targeted at *BCP* status

Recap

- Targeted at *BCP* status
- Provides background to explain:

Recap

- Targeted at *BCP* status
- Provides background to explain:
  - What is a *forged-origin sub-prefix hijack*?

Recap

- Targeted at *BCP* status
- Provides background to explain:
  - What is a *forged-origin sub-prefix hijack*?
  - Why *non-minimal ROAs* make such an attack easier/more effective?

Recap

- Targeted at *BCP* status
- Provides background to explain:
  - What is a *forged-origin sub-prefix hijack*?
  - Why *non-minimal ROAs* make such an attack easier/more effective?
  - Why use of `maxLength` often results in a *non-minimal ROA*?

Recap

- Targeted at *BCP* status
- Provides background to explain:
  - What is a *forged-origin sub-prefix hijack*?
  - Why *non-minimal ROAs* make such an attack easier/more effective?
  - Why use of `maxLength` often results in a *non-minimal ROA*?
- Recommendation: **don't do that**

Recent Updates

Section 3: **Example Hijack Description**

- Edited and re-ordered for readability:

See github issue #2

Recent Updates

Section 3: **Example Hijack Description**

- Edited and re-ordered for readability:
  - description of the sub-prefix attack with *loose ROA*

See github issue #2

Recent Updates

Section 3: **Example Hijack Description**

- Edited and re-ordered for readability:
  - description of the sub-prefix attack with *loose ROA*
  - specification of revised *strict ROA*

See github issue #2

Recent Updates

Section 3: **Example Hijack Description**

- Edited and re-ordered for readability:
  - description of the sub-prefix attack with *loose ROA*
  - specification of revised *strict ROA*
  - explanation of why sub-prefix attack is *mitigated*

See github issue #2

Recent Updates

Section 3: **Example Hijack Description**

- Edited and re-ordered for readability:
  - description of the sub-prefix attack with *loose ROA*
  - specification of revised *strict ROA*
  - explanation of why sub-prefix attack is *mitigated*
  - explanation of why prefix attack is still *possible but less likely* to attract traffic

See github issue #2

Recent Updates (cont.)

Section 4: **Measurements**

- Previous wording was *confusing* (at least to me)

Recent Updates (cont.)

Section 4: **Measurements**

- Previous wording was *confusing* (at least to me)
- New text is longer, but (hopefully) *clearer*

Recent Updates (cont.)

Section 4: **Measurements**

- Previous wording was *confusing* (at least to me)
- New text is longer, but (hopefully) *clearer*

Recent Updates (cont.)

Section 4: **Measurements**

- Previous wording was *confusing* (at least to me)
- New text is longer, but (hopefully) *clearer*

Questions for the working group:

Measurements are from 2017.

- Is there more recent data we should reference?

Recent Updates (cont.)

Section 4: **Measurements**

- Previous wording was *confusing* (at least to me)
- New text is longer, but (hopefully) *clearer*

Questions for the working group:

Measurements are from 2017.

- Is there more recent data we should reference?
- Is there any reason to believe the numbers have moved (much)?

Recent Updates (cont.)

Section 4: **Measurements**

- Previous wording was *confusing* (at least to me)
- New text is longer, but (hopefully) *clearer*

Questions for the working group:

Measurements are from 2017.

- Is there more recent data we should reference?
- Is there any reason to believe the numbers have moved (much)?

Recent Updates (cont.)

Section 4: **Measurements**

- Previous wording was *confusing* (at least to me)
- New text is longer, but (hopefully) *clearer*

Questions for the working group:

Measurements are from 2017.

- Is there more recent data we should reference?
- Is there any reason to believe the numbers have moved (much)?

See github issue #4

Recent Updates (cont..)

Section 5: **Recommendation Updates**

- Previous wording seemed to suggest that use of `maxLength` is bad in itself

See github issue #3 and issue #5

Recent Updates (cont..)

Section 5: **Recommendation Updates**

- Previous wording seemed to suggest that use of `maxLength` is bad in itself
- Emphasis should be on *attack-surface minimisation*

See github issue #3 and issue #5

Recent Updates (cont..)

Section 5: **Recommendation Updates**

- Previous wording seemed to suggest that use of `maxLength` is bad in itself
- Emphasis should be on *attack-surface minimisation*
- Re-worded to better reflect the intention:

See github issue #3 and issue #5

Recent Updates (cont..)

Section 5: **Recommendation Updates**

- Previous wording seemed to suggest that use of `maxLength` is bad in itself
- Emphasis should be on *attack-surface minimisation*
- Re-worded to better reflect the intention:
  - Avoid creating *non-minimal* ROAs

See github issue #3 and issue #5

Recent Updates (cont..)

Section 5: **Recommendation Updates**

- Previous wording seemed to suggest that use of `maxLength` is bad in itself
- Emphasis should be on *attack-surface minimisation*
- Re-worded to better reflect the intention:
  - Avoid creating *non-minimal* ROAs
  - Exercise caution to ensure that use of `maxLength` does not result in non-minimal ROAs

See github issue #3 and issue #5

Recent Updates (cont..)

Section 5: **Recommendation Updates**

- Previous wording seemed to suggest that use of `maxLength` is bad in itself
- Emphasis should be on *attack-surface minimisation*
- Re-worded to better reflect the intention:
  - Avoid creating *non-minimal* ROAs
  - Exercise caution to ensure that use of `maxLength` does not result in non-minimal ROAs
- Clarified that this approach creates difficulties whenever de-aggregation needs to happen fast (i.e. not only in the DDoS mitigation scenario)

See github issue #3 and issue #5

Recent Updates (cont..)

Section 5: **Recommendation Updates**

- Previous wording seemed to suggest that use of `maxLength` is bad in itself
- Emphasis should be on *attack-surface minimisation*
- Re-worded to better reflect the intention:
  - Avoid creating *non-minimal* ROAs
  - Exercise caution to ensure that use of `maxLength` does not result in non-minimal ROAs
- Clarified that this approach creates difficulties whenever de-aggregation needs to happen fast (i.e. not only in the DDoS mitigation scenario)
  - Better enumeration of the (bad) options that exist

See github issue #3 and issue #5

Recent Updates (cont..)

Section 5: **Recommendation Updates**

- Previous wording seemed to suggest that use of `maxLength` is bad in itself
- Emphasis should be on *attack-surface minimisation*
- Re-worded to better reflect the intention:
  - Avoid creating *non-minimal* ROAs
  - Exercise caution to ensure that use of `maxLength` does not result in non-minimal ROAs
- Clarified that this approach creates difficulties whenever de-aggregation needs to happen fast (i.e. not only in the DDoS mitigation scenario)
  - Better enumeration of the (bad) options that exist
  - We need a solution to this limitation of ROV

See github issue #3 and issue #5

Recent Updates (cont. . .)

Section 6: **RTBH Signalling**

- Previous versions were **over-stepping wildly!**

See github issue #6

Recent Updates (cont. . .)

Section 6: **RTBH Signalling**

- Previous versions were **over-stepping wildly!**
- Recommended a validation procedure that:

See github issue #6

Recent Updates (cont. . .)

Section 6: **RTBH Signalling**

- Previous versions were **over-stepping wildly!**
- Recommended a validation procedure that:
  - Conflicts with RFC6811

See github issue #6

Recent Updates (cont. . .)

Section 6: **RTBH Signalling**

- Previous versions were **over-stepping wildly!**
- Recommended a validation procedure that:
  - Conflicts with RFC6811
  - Is not implementable on most (all?) ROV-capable BGP speakers

See github issue #6

Recent Updates (cont. . .)

Section 6: **RTBH Signalling**

- Previous versions were **over-stepping wildly!**
- Recommended a validation procedure that:
  - Conflicts with RFC6811
  - Is not implementable on most (all?) ROV-capable BGP speakers
- Revised text:

See github issue #6

Recent Updates (cont. . .)

Section 6: **RTBH Signalling**

- Previous versions were **over-stepping wildly!**
- Recommended a validation procedure that:
  - Conflicts with RFC6811
  - Is not implementable on most (all?) ROV-capable BGP speakers
- Revised text:
  - *Acknowledges* that ROV and RTBH are not a good fit today

See github issue #6

Recent Updates (cont. . .)

Section 6: **RTBH Signalling**

- Previous versions were **over-stepping wildly!**
- Recommended a validation procedure that:
  - Conflicts with RFC6811
  - Is not implementable on most (all?) ROV-capable BGP speakers
- Revised text:
  - *Acknowledges* that ROV and RTBH are not a good fit today
  - *Punts* a solution to the underlying problem out of scope

See github issue #6

Recent Updates (cont. . .)

Section 6: **RTBH Signalling**

- Previous versions were **over-stepping wildly!**
- Recommended a validation procedure that:
  - Conflicts with RFC6811
  - Is not implementable on most (all?) ROV-capable BGP speakers
- Revised text:
  - *Acknowledges* that ROV and RTBH are not a good fit today
  - *Punts* a solution to the underlying problem out of scope
  - *Recommends* that RTBH-signalling mechanisms not require non-minimal ROAs

See github issue #6

Next Steps

The authors believe the draft is *ready to ship*

Questions?

Comments?

Praise?

WGLC please