Another Support for Multiple Hash Algorithms in Cryptographically Generated Addresses (CGAs)

(draft-zhou-6man-mhash-cga-00)

S. Zhou, R. Zhang, Z. Xie
IETF 83-6man, 2012-3
Motivation

- **Motivation:**
  - SHA1 is hardcoded in Cryptographically Generated Addresses (CGAs) define in RFC 3972
  - At most 3 hash algorithms will be supported in RFC 4982
  - But support of 8 hash algorithms is reasonable

- **Proposal**
  - Trying to support more hash algorithms (8)
  - An improvement to RFC 4982
CGA generation in RFC3972

```
Modifier+1

HASH2

16*sec=0?

N

 Modifier

0

Subnet prefix

Collision count

Y

 HASH2

N

 Modifier

0

Subnet prefix

Collision count

Y

 IPv6 address conflict?

N

64bits

16*sec=0?

N

 Modifier+1

0

Subnet prefix

Collision count

Y

 IPv6 address conflict?

N

64bits

Actually 64-3-2=59 bits
```
Solution in RFC 4982

- Hash indication must be in CGA to prevent down grading attack (RFC 4982)

- Shortened HASH1 output will weaken security level

- Redefinition of Sec in RFC 4982

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
<th>RFCs</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHA-1_0hash2bits</td>
<td>000</td>
<td>3972, 4982</td>
</tr>
<tr>
<td>SHA-1_16hash2bits</td>
<td>001</td>
<td>3972, 4982</td>
</tr>
<tr>
<td>SHA-1_32hash2bits</td>
<td>010</td>
<td>3972, 4982</td>
</tr>
</tbody>
</table>
Our proposal (figure)
Our proposal

- New extension field "Mhash-method"

<table>
<thead>
<tr>
<th>Extension Type</th>
<th>Extension Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mhash-method</td>
<td></td>
</tr>
</tbody>
</table>

mhash-method | Value
-------------+-------
4982         | 0
this draft   | 1

- New parameter “hid”

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHA-1</td>
<td>000</td>
</tr>
<tr>
<td>SHA-244</td>
<td>001</td>
</tr>
<tr>
<td>SHA-256</td>
<td>010</td>
</tr>
<tr>
<td>SHA-384</td>
<td>011</td>
</tr>
<tr>
<td>SHA-512</td>
<td>100</td>
</tr>
<tr>
<td>TBD</td>
<td>101</td>
</tr>
<tr>
<td>TBD</td>
<td>110</td>
</tr>
<tr>
<td>TBD</td>
<td>111</td>
</tr>
</tbody>
</table>
Security Consideration

- Overall security in RFC3972
  \( O(2^{(16\times\sec)+59}) \).
- Overall security in this draft
  \( O(2^{(16\times\sec)+3+56}) \).
Next Steps

- Improvements based on comments
- Ask for adoption as WG item

Thanks!