COSE: AES-CTR and AES-CBC

draft-ietf-cose-aes-ctr-and-cbc-01

Russ Housley and Hannes Tschofenig
Background

• The SUIT WG is using CBOR and COSE
• The SUIT WG is working on firmware encryption scheme, which is also expected to be used in TEEP
• IETF 114: Explained need for ciphers without integrity protection
  • Existing bootloaders use AES-CTR for firmware encryption
  • Lack of encryption expansion makes the job much easier
  • Signature over plaintext payload provides integrity protection
• This draft registers AES-CTR and AES-CBC
  • Only allowed in combination with a separate integrity mechanism
  • COSE WG adopted the draft on 11 Oct. 2022
## Proposed Algorithm Registrations

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
<th>Key Size</th>
<th>Description</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>A128CTR</td>
<td>TBD1</td>
<td>128</td>
<td>AES-CTR w/ 128-bit key</td>
<td>Deprecated</td>
</tr>
<tr>
<td>A192CTR</td>
<td>TBD2</td>
<td>192</td>
<td>AES-CTR w/ 192-bit key</td>
<td>Deprecated</td>
</tr>
<tr>
<td>A256CTR</td>
<td>TBD3</td>
<td>256</td>
<td>AES-CTR w/ 256-bit key</td>
<td>Deprecated</td>
</tr>
<tr>
<td>A128CBC</td>
<td>TBD4</td>
<td>128</td>
<td>AES-CBC w/ 128-bit key</td>
<td>Deprecated</td>
</tr>
<tr>
<td>A192CBC</td>
<td>TBD5</td>
<td>192</td>
<td>AES-CBC w/ 192-bit key</td>
<td>Deprecated</td>
</tr>
<tr>
<td>A256CBC</td>
<td>TBD6</td>
<td>256</td>
<td>AES-CBC w/ 256-bit key</td>
<td>Deprecated</td>
</tr>
</tbody>
</table>
Concerns about AES-CTR and AES-CBC

- Signature Stripping
- AES-GCM to AES-CTR authentication key compromise attack
- AES-GCM to AES-CTR malleability attacks
- AES-GCM to AES-CBC plaintext recovery attacks

Security Considerations text for each of these was proposed on the mail list
Possible Ways Forward

Options:

1. Proceed with the proposed security considerations text
2. Drop AES-CBC; proceed with the proposed AES-CTR security considerations text
3. Stop working on this document –
   a. Tell SUIT WG to figure out a way to use an AEAD
   b. At least some bootloaders will not use the SUIT solution