NIST Responses to Public Comments on Draft SP 800-38C
May 7, 2004

This document briefly summarizes the most significant public comments, and NIST's responses, on the September, 2003 draft of Special Publication 800-38C *Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality*. The comment summaries are numbered and set in bold; the author(s) of the comments are identified in parenthesis. The public comments are available through the modes of operation home page, http://nist.gov/modes.

1. Choose a better-engineered mode (Bellare, Barreto, Iwata, Rogaway, Wagner).

The wireless LAN industry appears to be committed to CCM, and, absent the identification of a significant security concern, NIST has decided to support the use of CCM within the IEEE 802.11 standard. NIST is open to recommending additional authenticated encryption modes.

2. Address Rogaway and Wagner's variable tag length attack (Struik).

In consultation with the CCM submitters, NIST decided that it was not necessary to adopt Struik's CCM* extension of CCM to address this concern. Instead, the specification now requires that the MAC length be fixed for each CCM key. Also, Appendix B now cites the attack in its description of the CCM authentication assurance.

3. Explain [remove] the recommendation for the 96 bit MAC length (Johnson, Kaliski) [(Struik)].

The guidance in Appendix B on the selection of the MAC length has been expanded, and the default recommendation for 96 bit MACs in Appendix B has been removed. For other MAC algorithms, some truncation of the MAC is prudent to hinder attackers from detecting collisions, but NIST has no evidence that this consideration applies to CCM.

4. Align MAC lengths with security levels (Johnson).

It could be misleading to align MAC lengths with symmetric key security levels, because MAC lengths are often targeted to prevent on-line attacks, while the security levels take into account off-line attacks too. For example, within an on-line session, 64 bit MACs are arguably consistent with 128 bit security against brute force key search; thus, in this case, 128 bit MACs may be unnecessarily conservative.

To handle this issue, in lieu of a safe default, the guidance in Appendix B on the selection of the MAC length has been expanded. In particular, a formula is given for selecting the minimum MAC length that is consistent with any desired limit on the probability of a breach of authentication, based on an estimate of an upper bound on the number of invalid purported ciphertexts that the system can accept during the lifetime of the key.

5. Restrict MAC lengths to multiples of 8 or 16 (Johnson).

The formatting function in Appendix A already restricts the MAC length to multiples of 16 bits between 32 and 128, so the comment presumably is directed at other formatting functions that may be developed in the future. Such restrictions, although sensible, are not in the spirit of flexibility that motivated the provision for such formatting functions. If necessary, option proliferation of any kind can be addressed at the level of the conformance tests themselves.

6. Address timing attacks on INVALID output (Kaliski).

The suggested text was added to the description of the decryption-verification process (Section 6.2).

7. Consider allowing the decryption-verification process to output the payload instead of INVALID if the authenticity is assured by some other method (Johnson).

This usage model is not covered in the CCM submission or the accompanying security analysis.

8. Consider allowing an option to disable authentication (Struik).

CCM without authentication, i.e., with MAC length of 0, is essentially the Counter mode, which is already approved. Thus, this suggestion amounts to allowing the use of CCM keys for pure Counter mode encryption, in violation of the principle of key separation. NIST does not see a benefit to this suggestion: authenticated encryption modes like CCM are intended to encourage and facilitate authentication where it otherwise might be engineered badly, or ignored altogether.

8. The option for alternative formatting function inhibits interoperability (Struik).

This is a common sort of tension in standards development. NIST expects that the specified formatting function will predominate in most applications of CCM. If, however, the specified formatting function turns out to have limited usefulness in practice, then alternatives should not be precluded.

9. Allow other integer representations (Struik).

If other integer representations are required for a particular application, then a new formatting function can be developed to accommodate them.

10. Clarify the upper bound on the number of block cipher invocations (Struik).

The upper bound was moved to the body of the document and worded as a requirement, as suggested.

11. The meaning of “sensitive but unclassified” data is not well settled (Hearne).

The phrase has been removed from the document.