Public Comments on
Draft Special Publication 800-38C

NIST received the following public comments on the draft Special Publication 800-38C, *Recommendation for Block Cipher Modes of Operation, the CCM Mode for Authentication and Confidentiality.*

Dr. Dworkin:

Thank you for soliciting comments on the draft version of NIST Special Publication 800-38C.

Your recommendation that the CCM algorithm be

> based on an approved symmetric key block cipher algorithm whose block size is 128 bits, such as the AES algorithm currently specified in FIPS Pub. 197

and that it not use

> the Triple Data Encryption Algorithm [3], whose block size is 64 bits

certainly makes sense.

However, I think you're stirring up a hornets' nest by stating in the Abstract that

> CCM may be used to provide cryptographic protection for sensitive, but unclassified, computer data.

(And the description of your recommendation at http://csrc.nist.gov/publications/drafts.html is even more prescriptive, i.e.

> the CCM mode of the Advanced Encryption Standard (AES) algorithm is specified for the protection of sensitive, unclassified data.

)

The question of what constitutes "sensitive but unclassified" information and, by inference, computer data within the U.S. Government is far from settled (see Genevieve Knezo's monograph, "Sensitive But Unclassified" and Other Federal Security Controls on Scientific Information: History and Current Controversy, at http://www.ieeeusa.org/forum/REPORTS/RL31845.pdf for a superb exegesis of the subject). The intrusion of that dispute into your otherwise laudable recommendation will, I fear, only vitiate its effectiveness. If a justification for CMM needs to be explicitly declared, might it not be better simply to state that it is "not intended to be used as a means for the protection of information meriting classification under the terms of E.O. 12958, as amended," or something equally amorphous? It would then remain the prerogative of an individual department or agency to choose to utilize CMM, or some other cryptographic mechanism, in order to protect such of its information which does not meet the definition for classified information.

If you'd like to discuss this, please feel free to contact me. In any event, thank you for writing a sound and lucid recommendation.

Yours truly,

Charles A. Hearne

Chuck Hearne

Engineer/Scientist
Information Assurance
Strategic Architecture
Integrated Defense Systems
THE BOEING COMPANY

The CCM mode has already been carefully and extensively evaluated, by Phil Rogaway and David Wagner, and their critiques provide numerous sound reasons why it is not the best choice for a standard. Their critiques can be found at:

http://www.cs.ucdavis.edu/~rogaway/papers/ccm.html

I suggest these be viewed as public comments for the proposed standard.

There are several alternatives to CCM which in my view are superior. One is EAX:

http://eprint.iacr.org/2003/069/

another is CWC:

http://eprint.iacr.org/2003/106/

Regards,

-Mihir Bellare

NIST,

A few comments on your recent CCM mode proposal:

1. The MAC size should always be a multiple of 8 bits (and maybe 16 bits), regardless of what is decided based on other comments below and from others. This at least limits the amount of possibilities that need to be tested for implementation conformance.

2. It is not clear why the specification says that only INVALID is returned on an error. Certainly the security of the method should not depend on this being the case. There can be reasons to issue the plaintext in some cases even if the MAC fails, for example, if there is some other way to determine integrity. ANSI X9 says that if a normal MAC fails, then this the message has not been authenticated by the MAC and it does NOT mean that the message is invalid (for example, perhaps the MAC got a bit flip). In particular, a message MIGHT be authenticated by some other means.

3. It is not clear why a 96 bit MAC was chosen at the interoperability choice. This does not conform to ANY of the 3 security levels announced by NIST of 80, 112, and 128 bits. Mapping directly to the 3 security levels would seem to be the most natural mapping. For bandwidth/performance concerns analysis is needed but possible, as pointed out.

4. It is also not clear why 64 bits was specified as the minimum MAC size to use without analysis, this might encourage users to converge on that, but it may not be appropriate. For example, as the trial MAC attack is probabilistic, some applications would need very low chances of a lucky guess if they have high security assurance requirements. The safe default is that anything lower than the desired security level needs analysis.

Don B. Johnson
Security Consultant
CygnaCom Solutions, Inc.
an Entrust company

Reading the draft, I noticed a typo:

On page 10 of the draft in section 5.4 Input Formatting :
in property 2. the last words should probably read i<=r and i<=s

Regards,

Ferenc Rakoczi
Sun Microsystems

Dear NIST team,

I must admit the proposal to standardize the CCM mode of operation is quite surprising. It would seem that any NIST-approved mode of operation should be equally applicable to any NIST-approved block cipher. This certainly does not hold for CCM, which is only defined for 128-bit block ciphers -- that is, one can use CCM with AES, but not with Triple DES nor Skipjack.

Since there are alternatives not hindered by the limitations of CCM (for instance, the EAX mode described in <http://eprint.iacr.org/2003/069/>), it would seem sensible to consider them as well. A very interesting analysis of CCM is available at <http://eprint.iacr.org/2003/070/>.

Best regards,

Paulo S. L. M. Barreto.
Chief Cryptographer.
Scopus Tecnologia S.A.

Dear NIST modes of operation team,

I would like to submit comments on the NIST draft SP800-38C.

After reading Phillip Rogaway and David Wagner's
analysis ``A Critique of CCM'' carefully,
I concur with their analysis, and I agree with their
conclusions. I feel that CCM is not the best choice
for a general-purpose standard.
I believe EAX and CWC are superior than CCM.

Best regards,

Tetsu Iwata
Ibaraki University

Dear Morris,

Thanks for posting the CCM mode as a proposal for a standardized authenticated encryption mode. There is a need for standards in this area, and NIST is well-positioned to lead the way.

As many of your correspondents have already noted, the paper at http://eprint.iacr.org/2003/070/ gives well-founded reasons for considering that CCM is not the optimal solution for an authenticated encryption mode. (For example, CCM requires that the encrypter knows the length of the message in advance, making encryption of an indeterminate-length stream difficult unless the stream is split into fixed-length blocks at the application level). Other designs, such as the EAX or OCB mode, should certainly be considered for standardisation.

However, NTRU considers that CCM should also be included in a NIST standard, because it is currently being baked into many higher-level standards such as the IEEE 802 wireless networking standards family. CCM is considered secure, even by those who object to it on engineering grounds, and approving it as a mode would make it simpler for devices following these standards to gain FIPS approval. We would therefore encourage NIST to standardize both CCM and another, better engineered, authenticated encryption mode.

Best wishes,

William

==========

William Whyte
Director, Cryptographic R&D
NTRU Cryptosystems