Public Comments on CWC, GCM

June 2, 2005

This document contains the public comments, received as email messages, on NIST's announced intention to recommend either the CWC or the GCM.

Commenter	Date Received	Page
Doug Whiting	May 4, 2005	2
David L. Black	May 14, 2005	3
Larry Hofer	May 31, 2005	4

As one of the inventors/authors of CWC, I'd like to vote in favor of GCM in your current mode considerations. While I believe that both algorithms are similar in their performance and security characteristics, the fact is that GCM has already made its way into several standards. As a result, our company is actually designing GCM into next generation chips, while we are *not* doing so for CWC. I believe that it is in the best interest of everyone to rally around one standard.

Also, I heartily support your decision not to consider patented modes, which IMO would violate the spirit of the AES process.

Thanks
Doug Whiting
Chief Scientist, Hifn
dwhiting@hifn.com

Gentlemen,

I am the chair of the Fibre Channel - Security Protocols (FC-SP) working group of Technical Committee T11 (www.t11.org) that is working on security for Fibre Channel. I understand that "NIST intends to recommend a second combined mode for authentication and confidentiality, in particular, either the Galois Counter Mode (GCM) or the Carter-Wegman + Counter (CWC) mode." (http://csrc.nist.gov/CryptoToolkit/modes/) The FC-SP working group strongly recommends that, unless significant security or technical issues are identified, that GCM be selected for the following reasons.

The FC-SP working group is developing an adaptation of the IPsec ESP protocol for Fibre Channel. Because Fibre Channel can be a multi-gigabit/second link, the working group believes that an efficient combined mode for AES is desirable. The application of GCM to ESP has been worked out by the IETF in the forthcoming Proposed Standard RFC based on:

"The Use of Galois/Counter Mode (GCM) in IPsec ESP"
<draft-ietf-ipsec-ciph-aes-gcm-00.txt>, November 2004

The FC-SP working group intends to use the same method.

To the best of my knowledge, no corresponding integration has been specified for CWC. Unless there are technical or security issues that require this to be done for CWC, the FC-SP working group strongly prefers to make use of the fully developed GCM work, and therefore strongly prefers that NIST recommend GCM.

Sincerely,
--David L. Black

David L. Black, Senior Technologist
EMC Corporation, 176 South St., Hopkinton, MA 01748
+1 (508) 293-7953 FAX: +1 (508) 293-7786
black_david@emc.com Mobile: +1 (978) 394-7754

Hello,
As one of the active members in the Fibre Channel Security Protocols standard (FC SP) if it is cryptographically acceptable to approve GCM with some restrictions on its usage (e.g. tag length, IV length, etc.) I believe that would rally both IPSec and FC around one standard.

I also support your decision to not consider patented modes in the interest of interoperability.

Thanks,
Larry Hofer
Staff - Office of the CTO, McDATA Corp.
larry.hofer@mcdata.com