Public Comments on Draft NIST Special Publication 800-38B
Recommendation for Block Cipher Modes of Operation:
The RMAC Authentication Mode

(Updated December 2, 2002)

NIST received the following public comments on the Draft NIST Special Publication 800-38B, *Recommendation for Block Cipher Modes of Operation: The RMAC Authentication Mode*.

Commenter	Date Received	Page
Tom Markham	October, 30, 2002	2
Small Business Administration	November 22, 2002	3
Department of Treasury	December 2, 2002	4

Tom Markham

The RMAC function looks very interesting and useful. This is a nice piece of work.

One of the obvious applications of the RMAC is to provide integrity checks for data packets such as those used in IPSEC. IPSEC uses Cipher Block Chaining and a block cipher. Currently IPSEC uses the HMAC function which requires IPSEC devices to implement both SHA-1 and a block cipher. There are obvious advantages to combining the encryption function which provides confidentiality with the encryption function which provides the integrity check. I expect that the IETF will develop an Internet Draft which attempts to combine AES in CBC mode with AES in RMAC mode to produce an efficient transform for IPSEC packets.

NIST could provide a service to the security community by adding an appendix to the RMAC publication which provides NIST guidelines for combining CBC with the RMAC function. This could include guidelines for generation and use of Initialization Vectors/SALT and potentially generation of the entire set of keys. e.g. can the IV also serve as the salt value or must the IV and the salt be separate.

The advantage of NIST doing this is that the transforms would be developed and reviewed by competent cryptographers.

Thank you

Tom Markham

SBA Comments on Draft NIST Guideline 800-38B - Recommendation for Block Cipher Modes of Operation: The RMAC Authentication Mode

1. The document did not include Power Measurements and Energy Efficient Implementations of Network Security Algorithms for Wireless Sensor Networks. Here is the summary for power measurement:

   - **The average energy consumption of Diffie-Hellman key agreement is 2.24 Joule in 5.75 second.**
   - **The average energy consumption of Rijndael encryption standard is 0.38 m Joule in 1 m second.**
   - **Execution time and energy consumption of key set up and encryption differ in a factor of 1000.**

2. The manner of development is actually critical o the creation of a strong algorithm.

3. This document is applicable for implementing of PKI and digital signature infrastructure in near future for SBA.

4. With the value of *k* at a maximum of 256 for AES algorithm / 168 for Triple DES, I am not convinced this cryptographic methodology will remain secure for more than 24-48 months from implementation. Advances in processing speed, and assuming the target data stream is accessible to intercept and analysis, this would enable a brute force cracking within days at an average maximum resolution of 2 to the 64th iterations.

Consolidated comments from the Department of the Treasury are provided below.

1. Page 8, section 5.2, 5th paragraph line 5. "When r?0". Presume the "?" should be an operator, but have no idea which one.

Carol Ann Widmayer

Department of the Treasury

CIO

Enterprise IT Security Planning and Assurance