

Re: David's authenticated encryption mode.

## Re: David's authenticated encryption mode.

---

*Source:* <http://www.derkeiler.com/Newsgroups/sci.crypt/2006-08/msg01632.html>

---

- *From:* "Tom St Denis" <[tomstdenis@xxxxxxxxxx](mailto:tomstdenis@xxxxxxxxxx)>
  - *Date:* 29 Aug 2006 16:13:37 -0700
- 

David Gothberg wrote:

Tom St Denis wrote:

It looks nice, but my concern is that an attacker can learn the intermediate values of  $H[0]$ ,  $H[1]$ , etc before the final output. Will that affect the security of the MAC?  
Tom

Thanks for thinking it looks nice. And yes, that the attacker can guess some of the intermediate hashes probably is the main concern. I am no cryptanalyst, but as far as I understand it should not be a problem for several reasons:

Look at it a bit more carefully.

The key for the last encrypt is actually

$\text{Key} \text{ xor } 2 \text{ xor } m1 \text{ xor } E(m1) \text{ xor } H0 \text{ xor } \text{Key} \text{ xor } 3$

The keys cancel out and we know  $2 \text{ xor } 3 \text{ xor } m1 \text{ xor } H0$  [since we know  $m1$  and  $H0$ ] So the unknown bit of the key for the last encrypt is merely  $E(m1)$ . I still think it's a bad idea to know the intermediate values of the chained MAC.

Also the key xors outside the encrypt don't contribute anything since they cancel out.

$H0 = E_{\{\text{key} \text{ xor } H-1\}}(m0) \text{ xor } m0$

$H1 = E_{\{\text{key} \text{ xor } H0\}}(m1) \text{ xor } m1$

etc...

Should be enough, at least for a hash.

Aside from all this keep in mind you are invoking the key schedule for every block. Few ciphers are efficient in that model.

Re: David's authenticated encryption mode.

Re: David's authenticated encryption mode.

Tom

.