

## Re: Combining Hashes

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2005-02/0408.html>

---

**From:** unmanarc ([aaron\\_at\\_synacksecurity.com](mailto:aaron_at_synacksecurity.com))

**Date:** 02/19/05

To: bugtraq@securityfocus.com

Date: Sat, 19 Feb 2005 00:54:56 -0400

El Vie 18 Feb 2005 11:24, Kent Borg escribió:

- > *Concatenating two different hashes, for example SHA-1 and MD5,*
- > *apparently does not add as much security as one might hope.*
- >
- > *What about more complicated compositions? For example, a reader*
- > *comment posted on Bruce Schneier's blog*
- > *([http://www.schneier.com/blog/archives/2005/02/sha1\\_broken.html](http://www.schneier.com/blog/archives/2005/02/sha1_broken.html))*
- > *suggests the following:*
- >
- >  *$d1=SHA-1(data)$*
- >  *$d2=MD5(data)$*
- >  *$d3=SHA-1(d1+data+d2)$*
- >
- > *The final digest would be  $d1+d2+d3$*
- >
- > *(where "+" is concatenation)*
- >
- >
- > *I admit I don't know why this might be significantly better than*
- >  *$d1+d2$ , I was hoping someone here would.*
- >
- >
- > *-kb*

Having  $d1+d2$  may leave some useful information in order to obtain a collision more fastest because we can intersect these functions...  $SHA-1(d1+data+d2)$  is relative better than  $d1+d2$ . I dont think that is really secure...  $d2$  or  $d1$  may leave some useful information. we need to study and probe that.

I dont recomend something as:  $HASH(HASH(data)+data)$  until a research of propietaries of that where investigated and mathematical proved. The better method (i think) is:  $HASH(HASH(data))$ , because adds two layer... and have the same or more security than  $HASH(data)$ . it's simple... if you use  $HASH(data)$ , you can obtain  $HASH(HASH(data))$ , and crack from  $HASH(HASH(data))$  (if 2-ble round hash is more weakness).

## SecurityFocus Bugtraq: Re: Combining Hashes

A simple probe of a very basic crypto-system that isn't good idea have two rounds are: XOR, the second round leave the original text. With one way functions may happen something similar.

- 
- application/pgp-signature attachment: stored