

Re: Report of collision-generation with MD5

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2004-08/0066.html>

From: Borja Marcos (*borjamar_at_sarenet.es*)

Date: 08/19/04

Date: Thu, 19 Aug 2004 10:16:37 +0200

To: freebsd-security@freebsd.org

On 18 Aug 2004, at 20:08, Claudiu wrote:

> *hello,*

>

> *please explain what do you mean by "reverse the hash". Is this the*

> *recreation of the original message from its hash ?*

You cannot reverse a hash. By definition, it is a non-reversible mathematical function.

If you get a set of messages and apply a hash to each of them, given a big enough set of messages you will find that some of them have the same hash. The issue is not the existence of collisions. It is obvious that there will be collisions. The issue is how easy or hard it is to find a collision.

Imagine a very simple hash: a checksum. Given a message, M, it is trivial to generate another message with the same checksum. However, using a "cryptographically secure" hash, there is no easy method to do that, other than brute force.

What researchers have discovered could lead to a shortcut, easier (and cheaper) to perform than a brute force search for collision finding. It does not mean that those digests are "broken", but indeed it means that they are less secure than previously thought.

Borja.

freebsd-security@freebsd.org mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-security>

To unsubscribe, send any mail to "freebsd-security-unsubscribe@freebsd.org"