

Re: Now that SHA-1 is cracked...

Source:

<http://www.tech-archive.net/Archive/Exchange/microsoft.public.exchange2000.connectivity/2005-02/0110.html>

From: Paul Adare (padare_at_newsguy.com)

Date: 02/22/05

Date: Mon, 21 Feb 2005 20:33:57 -0500

In article <e4RayUHGFHA.560@TK2MSFTNGP15.phx.gbl>, in the microsoft.public.windows.server.security news group, Galen <galennews@gmail.com> says...

> *From Google:*

>

> *SHA-1 cracked!:*

> <http://www.techspot.com/story17011.html>

>

> *Perhaps the OP has been reading the news?*

>

Irresponsible journalism at its worst, and you obviously don't know enough about cryptography to understand the issues here. SHA-1 has not been cracked, the researchers have simply determined that rather than finding collisions in 2^{80} they can find them with 2^{69} . While that is 2048 times easier to find a collision, SHA-1 has not been cracked at all. I'd suggest that rather than reading the news you spend some time researching cryptography.

--

Paul Adare

"On two occasions, I have been asked [by members of Parliament], 'Pray, Mr. Babbage, if you put into the machine wrong figures, will the right answers come out?' I am not able to rightly apprehend the kind of confusion of ideas that could provoke such a question."

-- Charles Babbage (1791-1871)