

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

Source:

<http://www.tech-archive.net/Archive/Exchange/microsoft.public.exchange2000.connectivity/2005-02/0119.html>

From: Matt Gibson (mattg_at_blueedgetech.ca)

Date: 02/22/05

Date: Tue, 22 Feb 2005 09:56:49 -0800

Agreed.

Matt Gibson – GSEC

<thurberk@cscsw.com> wrote in message
news:1109084384.464291.145630@c13g2000cwb.googlegroups.com...
> *Matt Gibson wrote:*
> <snip A and B>
>> *C) Say the paper is right, and they can now break SHA-1 in ~2⁵³*
> *attempts.*
>> *What does this mean to most people? Nothing. With these attacks,*
> *you*
>> *cannot just get "I will give you 1 million dollars" to "I will give*
> *you 10*
> *million dollars". You'd have a better chance of getting*
> *"09sdfkj3uih3wi8"*
>> *to hash to the same value.*
>
> *Certainly true--this alleged vulnerability has no measurable effect on*
> *signed messages. However and unfortunately, some applications use*
> *SHA-1 as a more basic building block of their security. The most*
> *common example, of course, is storing the hash of a password in an*
> *accessible xml file, and authenticating the user if a hash of his input*
> *matches the hash in the xml file. Assuming that the Chinese can do*
> *everything they claim, and that the padding problem can likewise be*
> *overcome, these collisions surely reduce the security of such*
> *applications by the advertised amount.*
>