

Re: Question about hashing implementation for authentication

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-02/4797.html>

From: Garrett Kajmowicz (garrett_at_garrett.dyndns.biz)

Date: 02/26/05

Date: Sat, 26 Feb 2005 16:01:50 -0500

> *Garrett Kajmowicz wrote:*

- > *For instance, MAC addresses are quite structured. If the attacker can guess*
- > *the manufacturer of your Ethernet cards (and I don't think it's that hard),*
- > *then 24 bits already go out the window.*

I'm well aware of issues with the listed hardware devices, and there are countless others which can be used (hard drive serial number just came to mind, possibly other such devices). Thank you for addressing it in this forum, however. In regards to CPU serial numbers, that was another example.

I'm looking more for comment on algorithm selection and data size. But thank you for taking the time to respond.

– Garrett Kajmowicz