Subject: Re: Serial Hashing, How Secure?
Posted by a000clown on Mon, 23 Feb 2009 06:07:11 GMT
View Forum Message <> Reply to Message

RoShamBo wrote on Sun, 22 February 2009 02:48raven wrote on Sun, 22 February 2009 05:09It's fairly secure. From what I recall, the serial hash is generated by the original serial being hashed twice via md5.

I'd say its pretty damn secure.

No, it's not secure at all. It's extremely trivial to fake a serial.

EDIT: Although it would be fairly difficult to retrieve the original, I suppose.
So you're saying if the hashed version of my serial was 1234 and someone knew this, it would be easy for them to tell the server 1234, but not easy for them to figure out the original. That right?