Subject: Reversing Hashing Algorithums
Posted by gibberish on Sat, 24 Apr 2004 17:20:07 GMT
View Forum Message <> Reply to Message

It has been stated several times that is is not possible to reverse a CRC hash to get back to the original file.

While in principal this is true, one theme that occurs repeatedly in encryption based technologies is that great care has to be taken in order to ensure some of the golden rules are not broken.

Generally hashes cannot be reversed simply because for any hash value there is a large (possibly infinite) number of possible source values.

This does not hold true when the length of the source text is known or known to be less than a given number. At this point there is a finite number of possible source keys, additionally given the length of the Renegade key it is likely that less than 10 possible source keys would be present for a given hash.

At a minimum a CRC based hash could be broken with a brute force attack, in order to retrieve the set of possible source keys.

Additionally the CRC hash has published flaws which means that a skilled cryptographer could probably do better than an brute force attack.

Subject: Reversing Hashing Algorithums
Posted by zunnie on Sat, 24 Apr 2004 17:25:51 GMT
View Forum Message <> Reply to Message

Who cares, even if Black Hand Studios or RenGuard could obtain my serial.
I wouldnt be bothered with it because i know they will not abuse it.

[zunnie]

Subject: Reversing Hashing Algorithums
Posted by IRON FART on Sat, 24 Apr 2004 18:43:00 GMT
View Forum Message <> Reply to Message

While you are probably right, I don't think that anyone is skilled enough to do something like that, and even less put the effort into it.

Subject: Reversing Hashing Algorithums
Posted by Dan on Sat, 24 Apr 2004 21:36:36 GMT
View Forum Message <> Reply to Message

Why would they even need 1000s of serials?

Subject: Reversing Hashing Algorithums
Posted by Crimson on Sat, 24 Apr 2004 23:09:06 GMT
View Forum Message <> Reply to Message

But it would be EASIER to generate serials and test them by logging into WOL with them if I or anyone else wanted one.

Subject: Reversing Hashing Algorithums
Posted by Blazer on Sun, 25 Apr 2004 02:12:17 GMT
View Forum Message <> Reply to Message

FFS I'm tired of hearing about this...why aren't you ragging on the creators of PunkBuster, which does pretty much the same thing as RenGuard and also uses a serial hash.

Do you know that your REAL serial (not encrypted in any way) is sent PLAINTEXT over the internet everytime you log into WOL? With the average of a dozen routers it passes through on the way there, omg so many chances for people to steal your serial!!!

Please stop making a big deal about this issue...the serial hashes are used for comparison for bans, they are not (and can not be reversed back to the orig serial). Yes its possible to brutce force one, but guess what, you can brute force nearly anything, including your windows password, ssh password, etc. If someone had the skills to break into the RG network servers, and intercept some hashed serials, why would they bother even doing that, they could just use a similar brute force technique with programs that WSE released to brute force your password directly from WOL, without ever having to touch one of our servers or hack into anything at all.

Please stop the doomsaying.

Subject: Reversing Hashing Algorithums
Posted by renegay3 on Mon, 26 Apr 2004 03:32:03 GMT
View Forum Message <> Reply to Message

Quote:But it would be EASIER to generate serials and test them by logging into WOL with them if I or anyone else wanted one.

And if would be EASIER to simple get a new serial if you get banned for cheating.....

Subject: Reversing Hashing Algorithums
Posted by jonwil on Mon, 26 Apr 2004 04:00:57 GMT
View Forum Message <> Reply to Message

Your renegade serial is just one of the different pieces of information we use to ban.
We also use IP address, username and <deleted for security reasons>

Subject: Reversing Hashing Algorithums
Posted by Try_lee on Mon, 26 Apr 2004 15:21:55 GMT
View Forum Message <> Reply to Message

I wanna know what was deleted!!!