Subject: This should alleviate your concerns...
Posted by Blazer on Tue, 06 Apr 2004 01:27:56 GMT
View Forum Message <> Reply to Message

v00d00 brought up a good example of explaining how a one-way hash cannot reveal the origional data.

Lets say you have a 5MB file, text file, video clip, whatever.
You can create a 32bit hex number of that file.

So stay with me...5MB file, big number that is a "signature" of that file.

Now lets say that I post that 32bit number on the internet. Can someone use it, and with a super computer or whatever, "decrypt" it back to the 5MB of data? NO. It is simply a numerical signature of some data, it is not some algorithmn that converts the data to some encrypted form that can be reverse engineered.

However, with this signature, you can use it for COMPARISONS, to validate the origional data, without knowing what the data is.

Simple example:
Some file Simpsons.mpg , a 50 MegaByte video file. You create a 32bit hash of it and get a hexidecimal number like "d1f9c69e".

Now you send that number "d1f9c69e" to me. I cannot use this number to recreate your 50MB simpsons episode, even with all the computers in the world. But if I want to verify later that the Simpsons.mpg you have is the same one that you had earlier, I can regenerate a hash of Simpsons.mpg and if I get d1f9c69e again, then I know its the same file.

This is the way RenGuard tests your serial. Its a one-way hash that allows comparisons only to pre-recorded values. There is no way to recreate your serial from the data, except an elaborate brute force attack of generating random serials, hashing them, and then comparing the results to see if the hash matches. Frankly Renegade serial numbers are of such length I doubt anyone would want to dedicate their computer for months on end to do that just to get someones $9 serial number...it would be like trying to recreate 5 seconds of that 50MB video file I talked about, not to mention the only "someones" who even have access to the hashes are the Renguard team. Also, no hashes are saved or recorded, unless they are used for a ban.

I hope this helps clear up any misconceptions about RenGuard accessing your serial numbers. We realize that not everyone is a CS major and a thorough explanation is needed.

As to whether it is illegal or not to access the serial, I don't see any issues as renegades banlist.txt has options to ban by serial EA has shown us they do not support this game and as far as they are concerned it all but doesn't exist. I seriously doubt they are going to spend thousands of dollars to sue a bunch of volunteers who are just doing a good thing (stopping cheats).

LONG story short:
1. Renguard does not steal your serial.

2. Renguard makes an un-reversable signature of your serial, which can be used for comparison only. It cannot be decrypted back to your origional serial...period.
3. These signatures are not even recorded anywhere, until and only while a ban using one is in place (hopefully bans on the RG system will be a rare occurance anyhow).
4. Is RG Illegal for doing anything at all with the serial? Its a grey area. If it was an active game that they cared about, probably a bad idea to do anything including using a logo without their permission. But since Renegade is a legacy game, with no support whatsoever, I'm not expecting anythign to happen to the RenGuard team any more than being sued for using the Renegade windows icon. At any rate, that is OUR problem...so enjoy playing Renegade cheat-free, and leave the legal ramifications to us.

If anyone has any questions or comments, I will be happy to respond to them.
