Subject: This should alleviate your concerns...
Posted by England on Tue, 06 Apr 2004 08:30:27 GMT

View Forum Message <> Reply to Message

Dantelets not forget what the post said originally, either way, you still call me an idiot for things that blazer & v00d00 just confirmed as possible.

no you can't decrypt it, but YES you could (with bruteforce) find the serial.

Quote:As you might be aware, RenGuard has been in beta testing for about a week now. In that time, we have changed and fixed dozens of usability feedback items and bugs, and improved error handling. RenGuard changes and improves every passing hour. The feedback from our testers has been excellent and useful.

As you might expect, ways have been suggested to get around RenGuard. Some ways we have already thought of and countered. Some ways we might not. Our beta testers and even most people who read these forums are smart enough, and care about Renegade enough to approach us privately with their concerns. We appreciate those people.

However, there are others who are not so smart and don't care about Renegade and the success of RenGuard. Those people instead decide to take an approach not unlike some script kiddies who terrorized Renegade back in the day and posted their suggested ways to get around RenGuard on their website and tell everyone about it, so that in their mind, we'd be forced to fix the problem. But what they didn't understand is that we have been and are addressing this and other possible exploits and we won't release until they are resolved. We are unwaveringly commmitted to you, the players of Renegade, and there is NOTHING we have ever done that should make you doubt that. Hundreds of dollars and hundreds of hours has gone into this product with only one motive, to stop cheating in Renegade.

On that note, the concern was also brought up that we might be wanting to STEAL your serial number. This is simply not true.

Here, some serial hashes for your enjoyment.

c30aeb22
19576f7
b7c648c8
9f48b277
1e29757c
bc1b2892

Quote:
http://www.watchguard.com/glossary/o.asp

one-way hash function
A mathematical process performed on data to produce a numeric result called a message digest,

which cannot be reversed to produce the original message.

See hash and message digest.

hash code
A unique, mathematical summary of a document that serves to identify the document and its contents.

message digest
A mathematical function used in encryption to distill the information contained in a file into a single large number, typically between 128 and 256 bits in length. Message digests are also known as one-way hash functions because they produce results where it is mathematically infeasible to try to calculate the original message by computing backwards from the result. Message digest functions are designed so that a change to a single character in the message will cause the message to result in a very different message digest number. Many different message digest functions have been proposed and are now in use; most are considered highly resistant to attack.

Please read and understand this definition of a hash. Not only do we have no use for your serial, but we couldn't get it if we wanted to from the information the client sends to us. The only reason we even want anything close to your serial is for banning purposes. As you can guess, there will be people who will do their best to continue to make our lives miserable. In order to stop them from interfering with our games and the new RenGuard network, it is necessary to find as many ways as possible to ban them from the servers so that they can't disrupt those of us who want to enjoy the game.

In conclusion, I want to apologize for the display of immaturity you may have seen on here earlier, some of which was on my part, and assure you that you have no reason to fear our intentions. If you have any concerns, please feel free to contact me or anyone on the team privately, or visit our new RenGuard support channel, #renguard_support, on irc.n00bstories.com IRC network.

I know a man with the algorythm