Subject: Re: crimson i have a question (not unban or anythin)
Posted by Kanezor on Thu, 29 Sep 2005 22:39:24 GMT
View Forum Message <> Reply to Message

danpaul88 wrote on Thu, 29 September 2005 16:08Weirdo wrote on Thu, 29 September 2005 21:52Altough I'm not sure with this serials if it will happen because of the limit, but it is possible that multiple serials have the same hash code.

I believe that Westwood would have thought of this, and would not allow the serial generator to make two valid serials with the same hash...

Can't say for sure though, perhaps someone from the RG team knows?

If Westwood/EA were to store every CD key that they generated, it would take up *quite* a lot of hard drive space. Conversely, if they were to also store every matching keyhash, it would take up anywhere from 1.5x to 3.0x (1.5x is actually worst case, since that would imply that they aren't compressing the CD keys as much as they could) of the drive space already taken up, depending on how they were to store the data. Then, on top of the hard drive space required, to check every single key every time a new key is generated to verify no collisions have occured would require a lot of CPU time.
I'm not saying it can't be done... just that it likely isn't.

Now, with that in mind, it is even more unlikely that a collision has or will occur ... the MD5 sum alone has a collision chance of approximately in the realms of 1 in 2^128. I don't know about you, but I don't think Westwood/EA has generated quite that many CD keys just yet.

I don't know the specifics of Westwood's CD key data, but in other products which I have worked with, there's some static data to specify the Product, some random PartA value. To assist in the prevention of third parties generating valid random keys for us, there is also usually a PartB value which is generated based on the data which "key 1" is. Only the author of the cd key (in this case, Westwood/EA) would have the algorithm to verify that PartB is the correct matching value for PartA. Then, those values (Product ID, PartA, and PartB, and any other values embedded into the key) are turned into human-readable format (eg, 1234-186723-1126-28346-128), sometimes with letters... sometimes not... sometimes case-sensitive, sometimes not. (On a side note, I *much* prefer extensively-long number-only CD keys when compared to short keys with letters mixed in, since I can type numbers-only quite rapidly using only one hand on the numeric keypad on my keyboard). Then, when you connect to the official network (in this case, WOL), your origional CD key is reported to the server you've connected to. The server is then able to decode/decrypt your CD key from human-readable format into the embedded Product (my guess is that EA's embedded Product is the Sku number you see in your registry), PartA, and PartB values. It's able to verify that the Product matches the game you're connecting with (in this case, C&C Renegade) and that PartB is the correct matching value for PartA. If it all matches up, you're allowed on.

Westwood online goes one step further and creates an MD5 checksum of your user-readable CD key to be able to uniquely identify you to any game server. Admins of the game server cannot decrypt the MD5 checksum in a feasable amount of time (one; the user-readable CD key is of a longer length than the MD5 checksum itself (22 bytes compared to 16 bytes), and two; generating

a rainbowcrack table for the entire namespace of Renegade cd keys would take months at the very least, let alone a shitload of hard drive space).

In any case, what I'm getting at is that usually the embedded data within your CD key is no longer than about 10-12 bytes (and thus, there can be no more than 2^80 to 2^96 possible human-readable CD keys, whereas there's 2^128 possible MD5 hashes). MD5 is a one-way checksumming algorithm (aka, hashing algorithm), and was created to evenly spread out the checksums. Generally, it will have near-zero collisions for any data shorter than 128 bit in length. Since the embedded data in C&C Renegade CD keys are likely shorter than 128 bits, the chances of collisions occuring are pretty much nil... and if one *does* occur, then EA can simply issue a new CD key to all parties involved.
