Subject: This should alleviate your concerns...
Posted by Crimson on Mon, 05 Apr 2004 23:50:50 GMT
View Forum Message <> Reply to Message

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 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.

Subject: This should alleviate your concerns...
Posted by bigejoe14 on Tue, 06 Apr 2004 00:05:51 GMT
View Forum Message <> Reply to Message

I trust anything and everything that comes from you guys. I know you won't let us down.

Subject: This should alleviate your concerns...
Posted by EnderGate on Tue, 06 Apr 2004 00:41:31 GMT
View Forum Message <> Reply to Message

True, the client sends the serial in an encrypted form...

But you can't have my hash either ...

Subject: This should alleviate your concerns...
Posted by snipesimo on Tue, 06 Apr 2004 00:51:14 GMT
View Forum Message <> Reply to Message

Same here.

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.

Subject: This should alleviate your concerns...
Posted by cowmisfit on Tue, 06 Apr 2004 01:38:56 GMT
View Forum Message <> Reply to Message

I completely 100% trust you guys, this program works people anyone who thinks they are doing anything other than to save rengegade your wrong ill tell you that right now. Anyone who is putting all this time, money into a mere game ecpecially adults really care.

Thanks Renguard Team for all the work you've completed and will do in the future, keep it up

---

Subject: This should alleviate your concerns...
Posted by v00d00 on Tue, 06 Apr 2004 02:53:39 GMT
View Forum Message <> Reply to Message

Something else I brought up in private, but will share now..

Even if it was feasable to reverse the CD-Keys

1) Why? It's obviously in use by someone.
2) Again, why? There are numerous CD key generators, and it's algorythm isn't very hard to follow. Using it, you could simply create a file of EVERY serial, and try em till you find a unique valid one. (ie: fire em at the WOL server (when it's up) till it OK's it).
3) Reversing the CRC (or even generating a list of ALL serials + CRC's of those to look up against) would take longer than to simply create the list of all serials without crc's, and validate online.

The keygens have been around since the beginning of Renegade. Yes, most keys it create won't work.. Some will. If you have that much time on your hands to try to 1) steal a key, or 2) generate a valid WORKING one, then you obviously don't care about Renegade (because instead of doing that, you could be PLAYING, or HELPING the community).

If you are really desperate for a valid key, do what I did.. BUY it. Hell, with it's price in stores currently, buy 10. I bought it (like all other C&C games) when it first came out at full price. Now

I've seen it in local stores for $5-10.

- v00d00

Subject: This should alleviate your concerns...
Posted by Dante on Tue, 06 Apr 2004 05:34:30 GMT
View Forum Message <> Reply to Message

lets 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.

Subject: This should alleviate your concerns...
Posted by v00d00 on Tue, 06 Apr 2004 05:38:33 GMT
View Forum Message <> Reply to Message

But again, so can anyone (even without the serial hashes).. Lets see, spend time creating the CRC's, or JUST create the serials.. Creating only the serials = alot faster, and can be done renguard or not.. Hmm..

Hell, lemme just generate a few billion serials, and I bet most people here would be on the list.

Besides, at this point renegade serials aren't a big issue.. The hot topic lately has been getting FDS serials lol.

- v00d00

Subject: This should alleviate your concerns...
Posted by gibberish on Tue, 06 Apr 2004 05:56:35 GMT
View Forum Message <> Reply to Message

This whole argument is totally mute.

When it comes down to it, it is all a matter of trust.

Unless you are prepared to disassemble every executable that someone gives to you, you have to trust that the author isn't going to do something bad to you.

For example we only have the Renguard Teams word that Renguard won't format the hard drive of anyone running Final Rengade. In most cases a program has the potential to do anything your user account has rights to do.

So if you are logged in with admin rights the program can format your hard drive. The same goes for serial numbers you either Trust that the Renguard team will not steal your number (or you don't), if you don't trust them don't install the client.

Subject: This should alleviate your concerns...
Posted by jonwil on Tue, 06 Apr 2004 07:38:04 GMT
View Forum Message <> Reply to Message

As I am the only one with full source code to the client (MAC has a copy as well but its out of date), I can say for sure that there is no trojans, hard-disk-formatting code or other nasties in there.
I would advise people not to run RenGuard inside a debugger (e.g. if you have SoftIce running in the background) because the protection will trigger on it and I dont know what the protection does in that case but other than that, nothing bad will happen.

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

Subject: This should alleviate your concerns...
Posted by jonwil on Tue, 06 Apr 2004 08:35:10 GMT
View Forum Message <> Reply to Message

Even if you knew the encryption or hashing algorithims used for RenGuard, you would still need to figure out the encryption keys.
Difficult, especially given that a new key is generated every time the program connects to a server.

Subject: This should alleviate your concerns...
Posted by Majiin Vegeta on Tue, 06 Apr 2004 10:22:00 GMT
View Forum Message <> Reply to Message

dont Care if it stole my serial. what they gonna do with it?? sell it?? omg!!

Subject: This should alleviate your concerns...

Posted by Blazer on Tue, 06 Apr 2004 10:39:53 GMT
View Forum Message <> Reply to Message

Yeah imagine how rich the RenGuard team will become! All we have to do is steal all 2000 renegade players serials, and sell them on ebay for $10 (thats twice what the game sells for in the store)! thats $20,000! WHOO-HOO Geo Metro here I come!

Subject: This should alleviate your concerns...
Posted by DarkFish on Tue, 06 Apr 2004 10:50:46 GMT
View Forum Message <> Reply to Message

Although you might be able to sell a few to gullible or stupid people, I feel that demand would quickly run dry....

Subject: This should alleviate your concerns...
Posted by Dogg on Tue, 06 Apr 2004 11:03:25 GMT
View Forum Message <> Reply to Message

The sick and stupid part about people worrying about their precious serial numbers is soooo sad it is beyond comprehension. I am telling every single player do not ever play in GameSpy Arcade if this worries you. NEVER...

Because you know what? CD Key banning is the default method in GameSpy when you get banned. What does this mean? If your so paranoid that Renguard is gonna send some hashes or whatever out, OMFG, you gotta realize what happens when you get banned in GSA...think about it...it bans your CD Key...again...it BANS YOUR CD KEY...the Server KNOWS what your CD KEY IS...it's in I dunno how many characters, 32 maybe...don't feel like counting to tell ya, but the server in the WESTWOOD designed program records it anyways...all moderators gotta do is type ban 3 and if your user 3, it records a encrypted version of your CD KEY to the server in a text file...you won't even know you were banned and that your serial was recored because GSA only verifies when you join if your banned and kicks you then, so you aren't autokicked and you are clueless that the server jsut recorded in some encrypted algorythm, your CD-Key...

So to spew paranoid jimberish about renguard is just a sad little pathetic way to hide behind your cheats that you need to feel superior....

Get over it...use Renguard when it's ready and stop cheating....if Westwood considers it secure, why the hell shouldn't the renguard team? Do you really think Westwood would let every server record every GSA serail number to violate it's out terms of use to let every server op sell or steal them...if so...leave...soon...because thats the way it works...

Man...cheaters can cry about anything to get a few more kills...

Subject: This should alleviate your concerns...

Posted by GTCien on Tue, 06 Apr 2004 12:16:57 GMT
View Forum Message <> Reply to Message

u still care about ur serial!?#

so i dont care about mines , if i "loose" it ill buy me a new one and i ll get new cds and the book!

so wheres the problem!?
of course u can use an invalid serial (only on GSA/ASE)

its even payfree! (lol)

Im sure there are several players with not "valid" keys...

Subject: btw...
Posted by jonwil on Tue, 06 Apr 2004 12:24:15 GMT
View Forum Message <> Reply to Message

The serial is not the only thing we use for banning u.
I wont say what else we are using but even if you get a new serial. you wont automatically be allowed back on the network.

Subject: This should alleviate your concerns...
Posted by JaLi on Tue, 06 Apr 2004 14:59:54 GMT
View Forum Message <> Reply to Message

Well i Don't really trust anyone on the internet at all thats the way you keep yourself safe in my opinion, but... i gotta say you gotta trust these guys & Ladies oops sry Crimson,Because at the end of the day without Renguard you might aswell just use your C&C Renegade discs as coasters, Because without this Anti Cheat programme for renegade the game will Surely die
so i say what have you got to lose? Trust them & play in a cheat free Zone or Don't Trust them & let the Game Die?
i know what i want do you?
yup Trust them & play in a Free Cheat Free Zone
So i gotta say bring it sooner than Later Thanksbtw guys for all your Hard work.
and i would willingly contribute a small token i:e cash towards your Expenses np just let me know.
Thanks JaLiPiN0

Subject: This should alleviate your concerns...
Posted by flyingfox on Tue, 06 Apr 2004 19:34:56 GMT
View Forum Message <> Reply to Message

I dunno m8, doesn't seem to be many cheaters around these dayz.

I'm not sure if GX is still hosting final renegade anyway, if they aren't then that's probably some of the reason there've been less cheaters around. That's not to say they aren't. But face it, last year it was like an outbreak when renguard began development, these days it's nothing like it was then. I'll be glad to play on renguard servers but the it really isn't going to feel any different except you've got a few Kb of memory running in the background and 2 less kiddies per game tossing out the accusations.

Subject: This should alleviate your concerns...
Posted by Blazer on Tue, 06 Apr 2004 22:50:14 GMT
View Forum Message <> Reply to Message

I would like to stress again too that renguard bans will hopefully be a rare occurance. Nobody will be banned unless we notice them trying to crash or exploit the system, and even then they will have a chance to explain themselves. RenGuards primary function is to stop cheating, banning is just an option for stopping people attacking the system itself. Server owners will not have ability to ban people from the entire network, but of course they can ban whoever they want from their own server for whatever reasons they might have.

Subject: This should alleviate your concerns...
Posted by snipesimo on Wed, 07 Apr 2004 00:02:49 GMT
View Forum Message <> Reply to Message

I came to this conclusion of trust, so what if the RG team somehow got my acutal serial. What are they going to do with 500 Renegade serials? Not to mention the fact that even if they sold it WOL still allows 4 people to be online with one serial at one time.

Subject: This should alleviate your concerns...
Posted by Majiin Vegeta on Wed, 07 Apr 2004 19:09:32 GMT
View Forum Message <> Reply to Message

drkhazeI dunno m8, doesn't seem to be many cheaters around these dayz.

I'm not sure if GX is still hosting final renegade anyway, if they aren't then that's probably some of the reason there've been less cheaters around. That's not to say they aren't. But face it, last year it was like an outbreak when renguard began development, these days it's nothing like it was then. I'll be glad to play on renguard servers but the it really isn't going to feel any different except you've got a few Kb of memory running in the background and 2 less kiddies per game tossing out the accusations.

ive not played many games in the past month but everytime i do i've banned somebody for final ren big heads etc.

Subject: This should alleviate your concerns...
Posted by flyingfox on Wed, 07 Apr 2004 19:24:25 GMT
View Forum Message <> Reply to Message

Then I would hasten to say you're either unlucky or I'm lucky. Cheating just isn't like it was, and that can only be a good thing.

Bring on the renguard. w00t w00t and all that.

Subject: This should alleviate your concerns...
Posted by jager852 on Wed, 07 Apr 2004 19:31:53 GMT
View Forum Message <> Reply to Message

they might know renguard is comming so they stop before they get banned by it.

or they got tired of shooting someone tru his big heads and blow vehicles in 2 shots.

either way they stopped with cheating or playing renegade and for me that's a good thing .