Subject: RenGuard - Reverse Engineering
Posted by v00d00 on Wed, 15 Oct 2003 10:54:05 GMT
View Forum Message <> Reply to Message

A question regarding RenGuard. Because it's a client/server application, what will stop the legions of people who cheat, and can crack apps, from reverse engineering it down to it's core protocol / encryption (which I'll assume it has), and duplicating it, so that they have their own client which responds to the server with all the correct info for an unpatched Renegade, but in fact is patched.

Personally, I think you should write a server-side only anti-cheat, which hooks the networking routines in Renegade. From there, using either the help of your staff who worked on creating Renegade, or from knowledge aquired while working with the network code in Renegade, create a system to monitor hit locations (did they REALLY hit, based on calculations by the anti-cheat (stopping BH)), how much damage are they claiming, vs how much damage their currently selected weapon really does, etc.

Then, add rate-of-fire checking, complete w/ lag tolerance (since lagged client will of course, upon delag, seem to fire faster, etc), and option to simply "edit" the incoming packets, to filter out the cheat (reduce damage, stop bullets, etc), or kick-ban the cheater (admins decision, based on anti cheat config).

Is it just me, or does that make more sense?

The flaw to Renegade of course, which is the core to the cheats, is that unlike most other games, Renegade lets the CLIENT decide hit locations, damage, RoF, etc. Vs others which say, "ok, the client fired their pistol along this trajectory. Did they hit something? How much damage did they do to that target if so. Report findings to clients".

My only concern, is that there will be alot more teams of people ripping apart the hard work of your small team, and undoing what you have done. Can you keep up writing fixes / completely rewriting the protocol to counter them once they have created their OWN complete anti-RenGuard client? If not, consider the server-side only method, and solve it once and for all, with the only version changes being to fix bugs, and not complete rewrites which will really piss admins off (if it takes this long for the initial, how long after the cheaters create their own client to counter it will your rewrite take to do?).

- v00d00