Subject: Reversing Hashing Algorithums
Posted by Blazer on Sun, 25 Apr 2004 02:12:17 GMT

FFS I'm tired of hearing about this...why aren't you ragging on the creators of PunkBuster, which does pretty much the same thing as RenGuard and also uses a serial hash.

Do you know that your REAL serial (not encrypted in any way) is sent PLAINTEXT over the internet everytime you log into WOL? With the average of a dozen routers it passes through on the way there, omg so many chances for people to steal your serial!!!

Please stop making a big deal about this issue...the serial hashes are used for comparison for bans, they are not (and can not be reversed back to the orig serial). Yes its possible to brutce force one, but guess what, you can brute force nearly anything, including your windows password, ssh password, etc. If someone had the skills to break into the RG network servers, and intercept some hashed serials, why would they bother even doing that, they could just use a similar brute force technique with programs that WSE released to brute force your password directly from WOL, without ever having to touch one of our servers or hack into anything at all.

Please stop the doomsaying.