[in]security

by Gary McGraw

When Does Security Cross the Line? : : :

Piracy has always been a problem in the computer gaming business, and game makers have justifiably gone to great lengths to thwart it. But new kinds of piracy and game-related computer crime are causing the game makers to push the limits to defend themselves and their players. Recently, they went too far.

ONLINE GAMING, REAL-WORLD CHEATING

The most popular massively multiplayer online game on the planet today is World of Warcraft from Blizzard Entertainment, a subsidiary of Vivendi Universal Games. Called WoW for short, 4.5 million people worldwide play it, and about 500,000 are active at any one time. Like other role-playing games, WoW involves building virtual characters, accumulating experience, and gathering virtual stuff. As it turns out, both the characters and their stuff can be sold on eBay, so those bits are worth real money.

Which leads to cheating. Cheaters accumulate virtual stuff so that they can sell it for a quick profit. They take advantage of programming bugs in online games to "dupe" items (create value from scratch), level up (gain experience very quickly without actually playing), and carry out other exploits.

INVADING PRIVACY TO DEFEAT CHEATS?

WoW has a two-pronged attack against cheaters. The first is to make rules against cheating and ban those who violate them. These are called the "Terms of Use," and they're administered according to a legally binding EULA. Nothing wrong with that. The second is to keep an eye on the PC running the WoW client to determine whether it's being used to cheat. This one is the problem.

If monitoring someone's PC sounds like spying to you, that's because it is. WoW includes embedded code called the Warden that reads all sorts of data from the gamer's PC. The WoW Warden was recently outed by security researcher Greg Hoglund (www.rootkit.com/blog.php?newsid=358). (Disclosure: Hoglund and I wrote *Exploiting Software* [Addison-Wesley, 2004] together.)

Besides monitoring the WoW processes and keeping track of DLLs running in its process space, the Warden pokes around into other processes. It reads the window text in the titlebar of every window and scans the code loaded for every process running on the computer (which it hashes and then compares against hashes of known cheat code). According to Hoglund, the Warden program sniffed e-mail addresses and Web site URLs he had opened at the time and also read the names of other programs he was running on his computer.

The Warden is a clear invasion of privacy. Blizzard claims not to have any designs to use the data it digs up for purposes other than security, but there's nothing really stopping the company from doing whatever it wants on the gamer's PC. Although the EULA does warn that Blizzard may monitor PC activities with the Warden (without stating what the Warden actually does), this information is buried in the small print that almost nobody ever reads.

Online WoW forums and Web sites are abuzz with the spyware controversy. Some people believe complaining about spyware like the WoW Warden is silly, pointing out that if someone is so worried about it they can just choose not to play. I disagree. Historically, monitoring activities lead very quickly to abuse, and what Blizzard is doing in the name of security presents an unacceptably slippery slope. The trade-off between personal liberty and security is an essential one that must be carefully negotiated. Blizzard doesn't need to read my e-mail, surf my URLs, or look into my non-Blizzard processes.

> "Blizzard doesn't need to read my e-mail, surf my URLs, or look into my non-Blizzard processes."

If we stand by and let a game company poke around on our PC in the name of security, who do you suppose will do it next?

Gary McGraw is CTO of Cigital, a software quality management consultancy. He is co-author of Exploiting Software (Addison-Wesley, 2004), Building Secure Software (Addison-Wesley, 2001), and Java Security (Wiley, 1996). Reach him at gem@cigital.com.