The continuing battle between people who offer a service and others who want to hack into the service

devblogs.microsoft.com/oldnewthing/20120704-00

July 4, 2012

Raymond Chen

In the history of the Internet, there have been many cases of one company providing a service, and others trying to piggyback off the service through a nonstandard client. The result is usually a back-and-forth where the provider changes the interface, the piggybacker reverse-engineers the interface, back and forth, until one side finally gives up. Once upon a time, there was one company with a well-known service, and another company that was piggybacking off it. (I first heard this story from somebody who worked at the piggybacking company.) The back-and-forth continued for several rounds, until the provider made a change to the interface that ended the game: They exploited a buffer overflow bug *in their own client*. The server sent an intentional buffer overflow to the client, resulting in the client being pwned by the server. I'm not sure what happened next, but presumably the server sent some exploit code to the client and waited for the client to respond in a manner that confirmed that the exploit had executed. With that discovery, the people from the piggybacking company gave up. They weren't going to introduce an intentional security flaw into their application. The service provider could send not only the exploit but also some code to detect and disable the rogue client. By an amazing stroke of good fortune, I happened to also hear the story of this battle from somebody who worked at the provider. He said that they had a lot of fun fighting this particular battle and particularly enjoyed timing the releases so they caused maximum inconvenience for their adversaries, like, for example, 2am on Saturday.

Reminder: The ground rules prohibit "trying to guess the identity of a program whose name I did not reveal."

Raymond Chen

Follow