How can I make a call into an elevated service without requiring an elevation prompt?

devblogs.microsoft.com/oldnewthing/20191017-00

October 17, 2019

Raymond Chen

A customer said that they had two applications running on the machine. The client application is running non-elevated, and the service application is running elevated. They want the client to be able to make calls into the service without making the user approve elevation prompts for each call.

They tried playing around with various flavors of `CoCreateInstance`, but they always ended up with an elevation prompt or a non-elevated server.

I double-checked that when they said that they had a “service application”, they meant that they had a classic Windows service.

It was, and the answer has been around for decades.

Create an RPC service endpoint and set the service to start on demand. As an additional protection, you can use ACLs to control who can access the service (if you want to limit it to specific users or groups). But you still must handle the case where the client has been compromised. There is sample code on MSDN showing how to do this.

The customer confirmed that the tutorial worked as advertised and meets their needs. In fact, they realized that the service would already be running at the time the client needed to connect to it, so they didn’t actually need the auto-start functionality, but it was nice to know that it was available.

Larry Osterman noted that another solution is to register their COM server with an AppID that specifies that it should run in a service. In that case, COM will auto-start the service when the COM object is created.

Raymond Chen

Follow